INSTITUTO DEL MAR DEL PERÚ

RESOLUCIÓN DIRECTORAL N° DE-222-2009

Callao, 22 de octubre de 2009

CONSIDERANDOS:

Que, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI, quien está encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, mediante la Resolución Ministerial N°224-2004-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana *"NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.1° Edición"*, en todas las Entidades integrantes del Sistema Nacional de Informática;

Que, mediante la Resolución de la Comisión de Reglamentos Técnicos y Comerciales N°001-2007-INDECOPI-CRT, de fecha 05 de enero de 2007, se aprobó 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. 2° Edición"*, en reemplazo de la Norma Técnica Peruana NTP-ISO/IEC 17799:2004;

Que, la Presidencia del Consejo de Ministros, mediante Resolución Ministerial N°246-2007-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana *"NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2° Edición"*, en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar la creación de la infraestructura de Gobierno Electrónico, por considerar la seguridad de la información, como un componente importante para dicho objetivo;

Que, tomando en cuenta que la información es un activo que, como otros activos importantes de toda organización, tiene valor y requiere en consecuencia una protección adecuada, dado el creciente ambiente interconectado de las organizaciones. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades;

Que, a tal efecto el Instituto del Mar del Perú, mediante Resolución Directoral N°DE-046-2009, de fecha 18 de febrero de 2009, conformó la Comisión de Trabajo para la implementación de 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", la misma que elaboró el "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información en el Instituto del Mar del Perú", tomando en cuenta dos aspectos importantes: 1) la naturaleza de la información científica y tecnológica que posee y produce y 2) que la seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, procedimientos, estructuras organizativas, plan de contingencia de software y hardware: el cual, cuenta con opinión técnica favorable de la Oficina de Planificación, Presupuesto y Evaluación de Gestión;

Que, en consecuencia, debe emitirse la Resolución correspondiente, aprobando dicho documento de gestión institucional, dado que la Institución dispone de un parque informático de hardware y software, archivos y sistemas informáticos distribuidos en sus diferentes unidades operativas, tanto administrativas como científicas, necesarias de evaluar, articular y proteger en función del avance de la tecnología de la información y de los sistemas de seguridad;

De conformidad con lo establecido en la Resolución Ministerial N°246-2007-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana *"NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición"* y estando a las facultades conferidas en el inciso g) del Artículo 19° del Reglamento de Organización y Funciones del Imarpe, aprobado mediante Decreto Supremo N°009-2001-PE;

Con la visación de las Oficinas de Planificación, Presupuesto y Evaluación de Gestión, de Asesoría Jurídica y de Administración y de la Unidad de Informática;

SE RESUELVE:

ARTÍCULO PRIMERO.- Aprobar el **"Código de Buenas Prácticas para la Gestión de la Seguridad de la Información en el Instituto del Mar del Perú - Imarpe"**, de conformidad con lo establecido en 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" y que en anexo forma parte de la presente resolución.

ARTÍCULO SEGUNDO.- Encargar a la Unidad de Informática la ejecución de las acciones necesarias que conlleven a la implementación del Código de Buenas Prácticas para la Gestión de la Seguridad de la Información del Imarpe.

ARTÍCULO TERCERO.- Disponer que la Unidad de Informática considere en los Planes Operativos Informáticos de cada Ejercicio Fiscal, las actividades necesarias para el cumplimiento de lo dispuesto en la presente Resolución; tales como, políticas de seguridad de la información, control en el acceso a los sistemas de información y plan de contingencia.

ARTÍCULO CUARTO.- Disponer que la Unidad de Informática 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, Comuníquese y Publíquese

INSTITUTO DEL MAR DEL PERU
IMARPE

GODOFREDO CAÑOTE SANTAMARINA
Director Ejecutivo

CODIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACION EN EL INSTITUTO DEL MAR DEL PERÚ - IMARPE

NTP-ISO/IEC 17799: 2007

COMISION PCSI

IMARPE - PERU

2009 - 2012

INDICE

INTRODUCCIÓN

¿Qué es la seguridad de la información?

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene. La seguridad de la información se caracteriza aquí como la preservación de:

a) su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;

b) su integridad, asegurando que la información y sus métodos de proceso son exactos y completos;

c) su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización.

¿Por qué es necesaria la seguridad de información?

La información y los procesos que la apoyan, sistemas y redes son importantes activos de la organización. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, tesorería, rentabilidad, cumplimiento de la legalidad e imagen Institucional.

Las organizaciones y sus sistemas de información se enfrentan, cada vez mas, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños

como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados. La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organizaciones externas también puede ser necesaria.

Los controles sobre seguridad de la información son considerablemente más baratos y eficaces si se incorporan en la especificación de los requisitos y en la fase de diseño.

¿Cómo establecer los requisitos de seguridad?

Es esencial que la organización identifique sus requisitos de seguridad. Existen tres fuentes principales.

1. La primera fuente procede de la valoración de los riesgos de la organización. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.

2. La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

3. La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

Evaluación de los riesgos de seguridad

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debería equilibrarse con el posible impacto económico, resultante de los fallos de seguridad. Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, sólo a partes de ella o incluso a sistemas de información individuales, a componentes específicos de sistemas o a servicios dónde sea factible, realista y útil. La evaluación del riesgo es una consideración sistemática:

a) del impacto económico que probablemente resulte de un fallo de seguridad, teniendo en cuenta las posibles consecuencias de pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos;

b) de la probabilidad realista de que ocurra dicho fallo a la luz de las amenazas y vulnerabilidades existentes, así como de los controles implantados. Los resultados de ésta evaluación ayudarán a encauzar y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implantación de los controles seleccionados para protegerse contra dichos riesgos. El proceso de evaluación de riesgos y selección de controles, puede requerir que sea realizado varias veces para cubrir diferentes partes de la organización o sistemas de información individuales.

Es importante, efectuar revisiones periódicas de los riesgos de seguridad y de los controles implantados para:

a) tener en cuenta los cambios de los requisitos y las prioridades de negocio de la organización;

b) considerar nuevas amenazas y vulnerabilidades;

c) confirmar que las medidas de control siguen siendo eficaces y apropiadas.

Deberían realizarse estas revisiones con distintos niveles de detalle dependiendo de los resultados de las evaluaciones previas y de los umbrales de riesgo que la gerencia está dispuesta a aceptar. Se suelen realizar las evaluaciones de riesgo primero a alto nivel, como

un medio de priorizar recursos en áreas de alto riesgo, y después en un nivel más detallado para enfocar riesgos específicos.

Selección de controles

Una vez que los requisitos de seguridad han sido identificados, deberían elegirse e implantarse los controles que aseguren la reducción de los riesgos a un nivel aceptable. Pueden elegirse los controles partiendo de este documento, de otros conjuntos de controles o de nuevos controles que pueden diseñarse para cubrir adecuadamente las necesidades específicas. Hay muchas formas distintas de gestionar los riesgos y este documento proporciona ejemplos de enfoques habituales. Sin embargo hay que reconocer que ciertos controles no son aplicables para todos los sistemas o entornos de información y pueden no ser de aplicación en todas las organizaciones. Por ejemplo, en el apartado 9.1.4 se describe como pueden segregarse ciertas tareas para evitar fraudes y errores.

Las organizaciones pequeñas podrían no segregar todas las tareas y necesitarían otras formas para conseguir el mismo objetivo de control. Por poner otro ejemplo, los apartados 10.7 y 13.1 describen como puede hacerse el seguimiento del uso del sistema y recogerse evidencias. Las medidas de control descritas como el registro de eventos podrían entrar en conflicto con la legislación aplicable, como la referente a la protección de la intimidad de los datos de carácter personal de los clientes o de los datos laborales.

Los controles deberían elegirse por su costo de implantación en relación con los riesgos a reducir y con las posibles pérdidas si se materializa la ruptura de seguridad. También es conveniente tener en cuenta factores no económicos como la pérdida de reputación.

Ciertos controles expuestos en este documento, pueden considerarse como principios que guían la gestión de la seguridad de la información, aplicables a la mayoría de las organizaciones. Estos se explican en más detalle en el siguiente punto denominado **"Punto de partida de la seguridad de la información"**.

Punto de partida de la seguridad de la información

Cierto número de controles se consideran principios orientativos que proporcionan un punto de partida adecuado para implantar la seguridad de la información. Se apoyan en requisitos legislativos esenciales o se considera la mejor práctica habitual para conseguir dicha seguridad.

Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden:

a) la protección de los datos de carácter personal y la intimidad de las personas (véase el apartado 13.1.4);

b) la salvaguarda de los registros de la organización (véase el apartado 13.1.3);

c) los derechos de la propiedad intelectual (véase el apartado 13.1.2).

Los controles que se consideran comunes para la mejor práctica habitual para conseguir la seguridad de la información comprenden:

a) la documentación de la política de seguridad de la información (véase el apartado 4.1);

b) la asignación de responsabilidades de seguridad (véase el apartado 5.1.2.2);

c) la formación y capacitación para la seguridad de la información (véase el apartado 7.2.1);

d) el registro de las incidencias de seguridad (véase el apartado 7.3.1);

e) la gestión de la continuidad del negocio (véase el apartado 13.1).

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos. Es conveniente señalar que pese a la importancia dada a los controles en este documento, la importancia de cualquier control debería determinarse a la luz de los riesgos específicos que afronta la organización. Por tanto y aunque el enfoque anterior se considere un buen punto de partida, no sustituye a la selección de controles basada en una evaluación del riesgo.

Factores críticos de éxito

La experiencia muestra que los siguientes factores suelen ser críticos para el éxito de la implantación de la seguridad de la información en una organización:

a) una política, objetivos y actividades que reflejen los objetivos del negocio de la organización;
b) un enfoque para implantar la seguridad que sea consistente con la cultura de la organización;
c) el apoyo visible y el compromiso de la alta gerencia;
d) una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo;
e) la convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados;
f) la distribución de guías sobre la política de seguridad de la información de la organización y de normas a todos los empleados y contratistas;
g) la formación y capacitación adecuadas;
h) un sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información y sugerir mejoras.

Desarrollo de directrices propias

Este código de buenas prácticas puede verse como punto de partida para desarrollar la gestión específica de la seguridad en una organización. Pueden no ser aplicables todas las recomendaciones y controles de este código. Incluso pueden requerirse controles adicionales que este documento no incluye. Cuando esto suceda puede ser útil mantener referencias cruzadas que faciliten la comprobación de la conformidad a los auditores y otros asociados de la organización.

1. OBJETIVO Y ALCANCE

El objetivo del presente documento es definir las actividades que nos permitan reducir los riesgos y los hechos indeseados involucrados para garantizar los atributos de la información del IMARPE.

La Unidad de Informática, entre las diversas funciones que tiene se encarga de desarrollar nuevos productos software que la institución requiera. Almacenar y asegurar los datos de la institución. Asegurar la operatividad de la red institucional tanto física como lógica. Asegurar que los sistemas en producción estén respaldados.

La Unidad de Informática debe garantizar la preservación de la confidencialidad de la información institucional, la integridad de la misma, así como también su disponibilidad.

2. TERMINOS Y DEFINICIONES

Los conceptos generales que se incluyen a continuación han sido tomados del documento del INEI que se indica como referencia en el presente documento.

- PRIVACIDAD: Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quien, cuando y que información referente a ellos se difundirán o transmitirán a otros.
- SEGURIDAD: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

  En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

  El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o subconjuntos de ellos.
- INTEGRIDAD: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el

software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

- DISPONIBILIDAD: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran la información y los activos asociados.
- DATOS: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

  En su forma mas amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.
- BASE DE DATOS: Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que lo utilizan.

  También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un sistema de gestión o de Administración de Base de Datos (Data Base Management System-DBMS).

  Las características que presenta un DBMS son las siguientes:

  - Brinda seguridad e integridad a los datos.
  - Provee lenguajes de consulta (interactivo).
  - Provee una manera de introducir y editar datos en forma interactiva.
  - Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.
- ACCESO: Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del Terminal.

- ATAQUE: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.
- ATAQUE ACTIVO: Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.
- ATAQUE PASIVO: Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.
- AMENAZA: Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.
- INCIDENTE: Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.
- GOLPE(breach): Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.
- GESTION DEL RIESGO: Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos que afecten a los sistemas de información.
- ACTIVO: Algo que tenga valor para la organización.

- CONTROL: Herramienta de la gestión del riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.
- PAUTA: Descripción que aclara que es lo que debe hacer y como se hace, con el fin de alcanzar los objetivos planteados en las políticas.
- INSTALACIONES DE PROCESO DE INFORMACION: Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena.
- SEGURIDAD DE LA INFORMACION: Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también, pueden ser consideradas.
- EVENTO DE SEGURIDAD DE INFORMACION: Es una ocurrencia identificada de un sistema, servicio, o red el 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.
- INCIDENTE DE SEGURIDAD DE INFORMACION: Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información.
- POLITICAS: Dirección general y formal expresada por la gerencia
- RIESGO: Combinación de la probabilidad de un evento y sus consecuencias
- ANALISIS DEL RIESGO: Uso sistemático de la información para identificar fuentes y estimar el riesgo
- EVALUACION DEL RIESGO: Proceso General de análisis y evaluación del riesgo.
- VALORACION DEL RIESGO: Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este.
- TRATAMIENTO DEL RIESGO: Proceso de selección e implementación de medidas para modificar el riesgo.

- TERCEROS: Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión
- VULNERABILIDAD: Debilidad de un activo o grupo de activos que pueden ser explotados por una o mas amenazas
- INFORMACION. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.
- ACTIVOS DE INFORMACION. Los activos de información son datos o información propietaria en medios electrónicos, impreso o en otros medios, considerados sensitivos o críticos para los objetivos del IMARPE.
- CLASIFICACION DE LA INFORMACION. Es el ejercicio por medio del cual se determina pertenece a unos de los niveles de clasificación estipulados a nivel corporativo. Tiene como objetivo asegurar que la información reciba el nivel de protección adecuado. La información debe clasificarse en términos de la sensibilidad y la importancia para la organización .
- PROPIETARIO DE LA INFORMACION. Es una parte designada de la organización, un cargo, proceso o un grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuales son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación pérdidas de la confidencialidad o destrucción deliberada, y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida.
- CUSTODIO TECNICO. Es una parte designada de la organización un cargo, proceso o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (Toma de copias de seguridad, asignar privilegios de: acceso, modificaciones, borrado) que el propietario de la información haya definido, con base en los controles de seguridad en la organización.
- USUARIO. Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la organización en papel o medio digital, físicamente o través de las redes de datos y los sistemas de información de la institución. Son las personas que utilizan la información para propósitos propios de su labor,

adecuados y que tendrán el derecho manifiesto de uso dentro del inventario de información.

- AUTENTICIDAD. Quien haya recolectado la evidencia debe poder probar que es auténtica.
- CADENA DE CUSTODIA. Registro detallado del tratamiento de la evidencia, incluyendo quienes, como y cuando la transportaron , almacenaron y analizaron, al fin de de evitar alteraciones o modificaciones que comprometan las mismas.

3. EVALUACION Y TRATAMIENTO DEL RIESGO

OBJETIVO. Identificar componentes críticos en la infraestructura, comprender la actual situación de seguridad y Desarrollar Políticas de Seguridad centradas en la información

3.1 Evaluando los riesgos de seguridad de la información

Las valoraciones de riesgos deben identificar, cuantificar, y deben priorizar los riesgos contra el criterio para la aceptación de riesgo y los objetivos pertinentes a la organización. Los resultados deben guiar y deben determinar la apropiada acción administrativa y la prioridad para gestionar el riesgo de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. El proceso de evaluar los riesgos y seleccionar los controles puede necesitar ser realizado varias veces para cubrir diferentes partes de la organización o los sistemas individuales de información.

La evaluación del riesgo debe incluir el enfoque sistemático de estimar la magnitud de riesgos (el análisis de riesgo) y el proceso de comparar los riesgos estimados contra el criterio de riesgo para determinar la importancia de los riesgos (la evaluación de riesgo).

También deben realizarse periódicamente las evaluaciones de riesgo para conducir los cambios en los requerimientos de seguridad y en la situación de riesgo, por ejemplo en los recursos, amenazas, las vulnerabilidades, los impactos, la evaluación del riesgo, y cuando los cambios significativos ocurren. Estas evaluaciones de riesgo deben

emprenderse de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debe tener un alcance claramente definido para ser eficaz y debe incluir las relaciones con las evaluaciones de riesgo en otras áreas, si es lo apropiado.

El alcance de la evaluación de riesgo puede ser para la organización entera, o partes de ella, un sistema de información individual, componentes del sistema específicos, o servicios dónde esto es factible, realista, y útil. Se discuten ejemplos de metodologías de evaluación de riesgo en ISO/IEC TR13335-3 (Las guías para la Gestión de la Seguridad de la información: Las técnicas para el manejo de Seguridad de la INFORMACIÓN).

3.2 Tratamiento de riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, la organización debe decidir el criterio para determinar si o no se pueden aceptar los riesgos. Por ejemplo, pueden aceptarse los riesgos si se evalúa que el riesgo es bajo o que el costo de tratamiento no es rentable para la organización. Las decisiones tomadas deben ser documentadas.

Para cada uno de los riesgos identificados, siguiendo la evaluación del riesgo se debe tomar una decisión de tratamiento del riesgo. Las posibles opciones para el tratamiento de riesgo incluyen:

a) aplicando los controles apropiados para reducir los riesgos;
b) aceptando los riesgos objetivamente y con conocimiento, asumiendo que ellos satisfacen claramente la política de la organización y los criterios para la aceptación de riesgo;
c) evitar riesgos no permitiendo realizar acciones que causarían la ocurrencia de los riesgos;
d) transfiriendo los riesgos asociados a empresas o instituciones externas, por ejemplo aseguradores o proveedores.

Para los riesgos dónde la decisión de tratamiento de riesgo ha sido aplicar los controles apropiados, estos controles deben seleccionarse y deben llevarse a cabo para cumplir con los requerimientos identificados por una evaluación de riesgo. Los controles deben asegurarse de que los riesgos son reducidos a un nivel aceptable teniendo en cuenta:

a) los requerimientos y restricciones de la legislación nacional e internacional y las regulaciones;

b) los objetivos organizacionales;

c) los requerimientos y restricciones operacionales;

d) el costo de implementación y operación respecto al nivel de riesgo que esta siendo reducido, y restante, permaneciendo proporcional a los requerimientos y restricciones de la organización.

e) la necesidad de equilibrar la inversión en la implementación y funcionamiento de los controles contra el daño que pueda resultar de las fallas en la seguridad de la información.

3.3 Implementación de controles de riesgo de seguridad

3.3.1 Análisis del Riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: la probabilidad, impacto y exposición del riesgo. Estos elementos permitirán al equipo coordinador categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y dedicarse principalmente a la administración de los riesgos más importantes.

3.3.2 Probabilidad del Riesgo

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio informático. Asimismo, la probabilidad debe

ser inferior al 100% o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

La probabilidad se puede entender también como la posibilidad de la consecuencia, porque si la condición se produce se supone que la probabilidad de la consecuencia será del 100%.

3.3.3 Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia.

Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto.

Para nuestro caso, clasificaremos el impacto con una escala del 1 al 4.

3.3.4 Exposición al Riesgo

La exposición al riesgo es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

3.3.5 Definición de Eventos Controlables y No Controlables

Como parte de la identificación de los riesgos, estos deben categorizarse en función a las acciones de prevención que pueden estar en manos de el IMARPE, o cuya ocurrencia no puede predecirse con antelación. Así tenemos que los eventos pueden ser:

Eventos Controlables, si al identificarlos podemos tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado.

Eventos No Controlables, cuando su ocurrencia es impredecible y únicamente podemos tomar acciones que permitan minimizar el impacto en el servicio.

Esta identificación se hará en la matriz de riesgo explicada a continuación.

3.3.6 Definición de la Matriz de Riesgo

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas del servicio, en tal sentido, resulta vital conocer el impacto del evento cuando este se presenta, por lo que resulta necesario cuantificar la misma, a efectos de ser muy objetivos en su análisis. El factor numérico asignado es directamente proporcional y va en ascenso con respecto al impacto o gravedad que su ocurrencia pueda generar sobre los diferentes alcances del servicio y se clasificarán de la siguiente manera:

IMPACTO	DESCRIPCION	VALOR
Poco Impacto	Pérdida de Información y/o equipamiento no Sensitivo	1
Moderado Impacto	Pérdida de información sensible	2
Alto Impacto	Pérdida de información sensible, retraso o interrupción	3
Gran Impacto	Información crítica, daño serio, patrimonial	4

Cuadro N °1: Cuadro de Impactos

PROBALIDAD DE OCURRENCIA	DESCRIPCION
Frecuente	Incidentes repetidos
Probable	Incidentes aislados
Ocasional	Sucede alguna vez
Remoto	Improbable que suceda

Cuadro N °2: Cuadro de Probabilidad de Ocurrencia

Asimismo, la probabilidad de ocurrencia de un evento resulta de gran importancia para determinar que tan posible es que dicho evento se presente en la realidad. La determinación de esta probabilidad se obtendrá de la

estadística recogida de los eventos que se hayan presentado a lo largo de la administración del servicio por otros proveedores, así como de información obtenida de otros planes de contingencia para servicios similares.

Exposición = Impacto X Probabilidad

Impacto

Probabilidad de Ocurrencia		Poco	Moderado	Alto	Gran
	Frecuente				
	Probable				
	Ocasional				
	Remoto				

Cuadro N °3: Exposición

Finalmente, después de haber ponderado y validado objetivamente las probabilidades de ocurrencia y los impactos asociados, se establecerán las políticas que se han de considerar para determinar cuales son aquellos eventos que formarán parte del Plan de Contingencia. Al respecto, dichas políticas se indican a continuación:

- Todo evento cuya calificación sea de "Gran Impacto: 4", será considerado obligatoriamente dentro del Plan de Contingencia.
- Todo evento cuya exposición al riesgo sea mayor o igual a 0.15 será también considerado en el Plan de Contingencia.
- Después de todo lo expuesto, se elaborará la "Matriz de Riesgo de Contingencia" en la cual se tendrá en cuenta todos los eventos susceptibles de entrar en contingencia, indicando su ponderación y categorización (controlable/ no controlable) para la elaboración del Plan de Contingencia. Asimismo, se utilizarán los siguientes tópicos como una forma de agrupar a dichos eventos:
  - Contingencias relacionadas a Siniestros
  - Contingencias relacionadas a los Sistemas de Información
  - Contingencias relacionadas a los Recursos Humanos
  - Plan de Seguridad Física

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Ponderación	Alerta	Categoría
Sub Factor. Riesgos relacionadas a Siniestros Potenciales						
	INFRAESTRUCTURA					
1	Incendio	0.05	4	0.20		C
2	Sismo	0.10	4	0.40		NC
3	Inundación por fuga de agua	0.01	4	0.04		C
4	Inundación por braveza del Mar	0.10	4	0.40		NC
5	Perdida total de la capacidad de operación - Sede central del IMARPE	0.01	4	0.04		NC
	SERVICIOS PUBLICOS					
6	Interrupción de energía eléctrica	0.10	4	0.40		NC
7	Falta de suministro de agua	0.01	3	0.03		NC
8	Interrupción de servicios de telefonía	0.01	3	0.03		NC
	EQUIPO					
9	Falla de grupo electrógeno	0.04	4	0.16		NC
Sub Factor. Riesgos relacionados a Sistemas de Información						
	INFORMACION					
10	Extravío de documentos	0.05	4	0.20		C
11	Sustracción o robo de información	0.05	4	0.20		C
	SOFTWARE					
12	Infección de equipos por virus	0.10	4	0.40		C
13	Perdidas de los sistemas centrales	0.05	4	0.20		C
14	Perdida del servicio de correos	0.01	2	0.02		C
15	Falla del Motor de la base de datos	0.05	4	0.20		C
16	Falla del sistema operativo	0.05	4	0.20		C
17	Indisponibilidad de software, ofimática	0.02	3	0.06		C
	COMUNICACIONES					
18	Fallas en la red de comunicaciones interna	0.05	4	0.20		C
	HARDWARE					
19	Fallas de equipos personales	0.05	2	0.10		C
	RECURSO OPERATIVOS Y LOGISTICOS					
20	Falla de Fotocopiadora e impresora	0.01	4	0.04		C
21	Carencia de Suministros	0.02	4	0.08		C
Sub factor: Riesgos relacionadas a recursos humanos						
	RECURSO HUMANOS					
22	Tardanzas consecutivas del Personal	0.05	4	0.20		C
23	Ausencia del personal de jefaturas y direcciones	0.05	4	0.20		C
24	Emergencia medica	0.01	4	0.04		NC
25	Accidentes de trabajo	0.04	4	0.16		C
26	Deshonestidad	0.05	4	0.20		NC

Sub factor: Plan de seguridad Física						
	INFRAESTRUCTURA					
27	Robo recurso operativos, equipos diversos y software	0.05	4	0.20		C
28	Acceso a lugares no autorizados	0.01	4	0.04		C
29	Sabotaje	0.05	4	0.20		NC
30	Vandalismo	0.02	4	0.08		NC
31	Actos terroristas	0.02	4	0.08		NC

Cuadro N °4: Matriz de de Riesgos de Contingencia

Nota: El color rojo de la alerta representa que el evento es altamente impactante en el servicio por lo tanto debe ser obligatoriamente controlado.

En la columna CATEGORÍA por cada evento, se considera la identificación de aquellos eventos Controlables (C), y No Controlables (NC).

En el cuadro presentado a continuación se resumen los eventos según la categorización de eventos controlables y no controlables:

Item	Eventos controlables
1	Incendio
3	Inundación por fuga de agua
10	Extravió de documentos
11	Sustracción de información
12	Infección de equipos virus
13	Perdidas de los sistemas centrales
14	Perdida del servicio de correo
15	Falla de motor de la base de datos
16	Falla del sistema operativo
17	Indisponibilidad del software, ofimática
18	Fallas en la red de comunicaciones internas
19	Fallas de equipos personales
20	Falla de fotocopiadoras e impresoras
21	Carencia de suministros
22	Tardanzas consecutivas del personal
23	Ausencia de personal de jefaturas y direcciones
25	Accidentes de trabajo
27	Robo de recursos operativos, equipos diversos y software
28	Acceso a lugares no autorizados

Cuadro N °5: Eventos Controlables

Item	Eventos no controlables
2	Sismo
4	Inundación por braveza del Mar
5	Perdida total de la capacidad de operación - Sede central del IMARPE
6	Interrupción de energía eléctrica
7	Falta de suministro de agua
8	Interrupción de servicios de telefonía
9	Fallas del grupo electrógeno
24	Emergencia médica
26	Deshonestidad
29	Sabotaje
30	Vandalismo
31	Actos terroristas

Cuadro N °6: Eventos no Controlables

4. POLITICA DE SEGURIDAD

4.1 Política de seguridad de la información

OBJETIVO: Dirigir y dar soporte a la gestión de la seguridad de la información. La alta dirección debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización (véase el inciso 5.1.1)

4.1.1 Documento de Políticas de Seguridad de la Información

Se determina tres tipos de política de seguridad que definen una jerarquía. Ello permite ir de lo más general a lo más específico. Los tipos considerados son:

- Política de Seguridad de la Información a Nivel Institucional.
- Políticas de Seguridad de la Unidad de Informática.
- Políticas de Seguridad de Sistemas de Información.

4.1.1.1 Política de Seguridad de la Información a nivel Institucional

a) Ámbito de Aplicación

Este conjunto de políticas son aplicables a todos los integrantes del Instituto del Mar del Perú – IMARPE, ya sean trabajadores con contrato indefinido, profesionales con contratos administrativos de servicios

(CAS), Personal nacional o extranjero por convenios o proyectos, practicantes, tesistas o cualquier otro integrante que guarde algún tipo de relación o contrato con la institución.

b) Políticas

Las Políticas Institucionales son las grandes reglas o pautas que deben ser aplicadas a usuarios determinados en el ámbito de uso del plan de contingencia y seguridad de la información y son: seguridad y propiedad de la información (cuadro N ° 7) y usos indebidos (cuadro N ° 8).

Seguridad y propiedad de la información

Ítem	Política	Responsabilidad
1	Mantener la confidencialidad de la información a los que se tenga acceso	Todo el personal del IMARPE que administre información deberá guardar la confidencialidad del caso
2	Salvaguardar la Seguridad de las claves de acceso a los sistemas de información	Todo el personal del IMARPE será responsable de la privacidad de sus claves de acceso
3	Garantizar el acceso mediante password a las computadoras personales y portátiles; y mantenerlos a buen recaudo	Toda persona del IMARPE que tenga acceso a una computadora portátil o una PC asignada para su uso deberá solicitar que se obtengan las copias de respaldo
4	Las cuentas de correo proveídos por la Institución solo deben ser empleadas para aspectos laborales	Todo el personal del IMARPE que tenga asignada una cuenta de correo no podrá, bajo ningún motivo, usar el correo electrónico para aspectos no laborales
5	Mantener las precauciones del caso al abrir archivos anexos a los correos electrónicos que se reciban	Todo el personal del IMARPE deberá evitar abrir mensajes y anexos a los mensajes que sean sospechosos
6	Todos los contenidos Institucionales son propiedad del Instituto del Mar del Perú, por tanto no se podrá disponer de ellos sin autorización previa de la autoridad competente	Todo el personal del IMARPE deberá evitar la difusión de los contenidos institucionales salvo previa autorización

Cuadro N °7: Seguridad y Propiedad de la Información

Usos Indebidos

Ítem	Política	Responsabilidad
1	El empleo de software malicioso o sospechoso	Todo el personal del IMARPE no podrá hacer uso de software malicioso. En el caso de dudas la Unidad de Informática brindara la asesoría del caso
2	El envío de mensajes de correo no solicitados	Todo el personal del IMARPE solo podrá enviar mensajes relacionados a los interesados evitando la difusión de mensajes no deseados.
3	Enviar mensajes a terceras personas a nombre de la institución que no estén referidos a las labores propias de la misma	Todo el personal del IMARPE solo podrá enviar mensajes relacionados a su responsabilidad. No podrá representar a la institución salvo que tenga el encargo de las autoridades
4	Empleo del correo electrónico para efectos políticos, comerciales o de cualquier índole que no este referido al quehacer del Instituto del Mar del Perú –IMARPE	Todo el personal del IMARPE deberá abstenerse, bajo responsabilidad, de enviar mensajes con carácter político, comercial, en general no relacionados a las labores diarias.
5	Empleo indiscriminado del tamaño del correo electrónico.	No se permite la difusión de correos múltiples que tengan anexos archivos de tamaño extremo.
6	No esta permitido el uso de Messenger	Todo el personal del IMARPE se abstendrá del uso del Messenger.
7	Distribuir información Institucional mediante cualquier medio ya sea este escrito o electrónico, sin la aprobación de la autoridad correspondiente	Todo el personal del IMARPE queda impedido de distribuir contenidos institucionales salvo encargo de las autoridades.

Cuadro N °8: Uso indebidos de la Información

A continuación se muestra los diferentes tipos documentos que se utilizan en la institución (Cuadro N °9)

Nro.	Documento	Actividad	Responsable	Núm Copias
1	Memorando	Comunicar e informar a: Alta dirección, direcciones y/o jefaturas y unidades operativas del IMARPE	Alta dirección, Direcciones y/o Jefaturas	Necesarias

2	Carta	Comunicarse con Personas externas (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación, ministerios y otros)	Alta dirección y la Unidad de Logística	Necesarias
3	Oficios	Comunicarse con entidades externas (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación , ministerios y otros)	Alta dirección, direcciones y/o jefaturas	Necesarias
4	Correo electrónico	Intercambio de información con entidades externas nacionales e internacionales (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación , ministerios y otros) y Alta dirección, direcciones y/o jefaturas y unidades operativas del IMARPE	Cada usuario que hace uso del servicio de correo	Necesarias
5	Informes	Informar a las entidades externas nacionales e internacionales (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación , ministerios y otros) y Alta dirección, direcciones y/o jefaturas y unidades operativas del IMARPE	Alta dirección, direcciones y/o jefaturas	Necesarias
6	Resolución	Resolución para convenios con entidades externas (proveedores, proveedores, asociaciones, comunidad científica, empresas, institutos de investigación y ministerios) , Normas internas, aprobación de normas, Directivas, y formación de comités de trabajos a nivel de las direcciones y/o unidades operativas del IMARPE	Alta dirección	Necesarias

Cuadro N °9: Documentos a nivel institucional

4.1.1.2 Política de seguridad de la Unidad de Informática

a) Ámbito de Aplicación

Este conjunto de políticas son aplicables al personal de la Unidad de Informática, a todo responsable de administrar servicios de red o

servidores, así como a los usuarios de los diversos servicios que se brinden.

b) Políticas

Las Políticas referidas a la Unidad de Informática aplicables a los usuarios determinados en el punto anterior son:

De las Copias de Respaldo

Ítem	Política	Responsabilidad
1	Se determinará mantenimiento adecuado de toda información bajo custodia	La Unidad de Informática en coordinación con la Unidad de Logística e Infraestructura propiciará los medios de almacenamiento de tecnología actualizada y el ambiente adecuado para el almacenamiento de los backups de seguridad
2	Se determinara un calendario para la obtención de las copias de respaldo de la información de los servidores	La Unidad de Informática establecerá los calendarios para la obtención de las copias de respaldo
3	Se determinara un registro rotulado de las cintas de respaldo, incluyendo fecha y el responsable de la operación	La Unidad de Informática deberá rotular las copias de respaldo. Para lo cual se ha diseñado un formato adecuado. Anexo 6
4	Se determinara un espacio adecuado en dos Sedes Institucionales para el almacenamiento de las cintas con las copias de respaldo: Sede Central del IMARPE, Av. Argentina, Laboratorios y Bics(Buques de Investigaciones científicas)	La Unidad de Informática se asegurara de almacenar las cintas no solo en un espacio seguro sino también libre de humedad, tanto en la sede principal así como en la sede de la Av. Argentina, Laboratorios y Bics(Buques de Investigaciones Científicas)
5	Las copias de respaldo deben ser revisadas periódicamente para garantizar su estado	El responsable de la seguridad y la Unidad de Informática deberá revisar las copias de respaldo para asegurar su buen estado

Cuadro N °10: Copias de respaldo de la información

De los Accesos a los Servidores

Ítem	Política	Responsabilidad
1	Se establecerá un calendario de modificación de passwords de administración de los servidores	La Unidad de Informática, en coordinación con los administradores de los servidores determinará el calendario para el cambio de passwords
2	Se determinara un espacio físicamente seguro y apropiado para la ubicación de los servidores	La Unidad de Informática evaluara periódicamente (cada tres meses) el estado de la seguridad donde operan los servidores institucionales
3	Se restringirá el acceso a la sala de los servidores	Los administradores de los servidores aseguraran el no ingreso de personas extrañas a las zonas donde operan los mismos.
4	Se garantizara el aire acondicionamiento adecuada de la sala de servidores.	La Unidad de Informática será responsable de monitorear el estado de los equipos de aire acondicionado
5	Se mantendrán actualizados los antivirus que protejan a los servidores	La Unidad de Informática deberá asegurar la provisión e instalación de los antivirus requeridos por los clientes y por los servidores
6	Se implantarán sistemas firewall, contra spam, contra spyware, etc.	La Unidad de Informática instalara un firewall y un sistema antispam

Cuadro N °11: Accesos a los Servidores

Del uso de Software

Ítem	Política	Responsabilidad
1	No se podrá instalar software de cualquier tipo. Solo la Unidad de Informática esta autorizada para ello	Todo el personal del IMARPE queda prohibido de instalar software en las maquinas que tengan asignadas para su uso. Todo nuevo requerimiento deberá ser informado a la Unidad de Informática para evaluar conjuntamente con el usuario y proponer la alternativa mas adecuada
2	Ninguna persona podrá efectuar	Todo el personal del IMARPE queda

	modificaciones a las configuraciones de las computadoras, salvo el personal de la Unidad de Informática y previa autorización de la autoridad competente	prohibido de efectuar modificaciones a las computadoras que tienen asignadas. La Unidad de Informática es la única autorizada para tal
3	No se deberá descargar ni instalar software proveniente de Internet. Sin la previa evaluación por la Unidad de Informática proveerá de los filtros adecuados para el cumplimiento de esta política.	Todo el personal del IMARPE queda prohibido descargar software de Internet, sin haber sido evaluado por la Unidad de Informática
4	Se deberá mantener actualizado el inventario de software Institucional	La Unidad de Informática con apoyo de la Unidad de Logística e Infraestructura deberá establecer los procedimientos que garanticen la vigencia y actualización del inventario de las licencias de software.
5	Se debe administrar el software propietario y libre que la Institución utilice a la luz de la información que brinde la Unidad de Logística	La Unidad de Informática es la responsable de la administración del software garantizando el uso de solo las licencias y libre que el IMARPE posea

Cuadro N °12: uso del software

De los Virus

Ítem	Política	Responsabilidad
1	La Unidad de Informática mantendrá actualizados los antivirus instalados en las computadoras que conforman el parque informático institucional Las autoridades competentes brindaran las facilidades del caso para que el personal de la Unidad de Informática cumpla con esta disposición	Monitorear las computadoras para asegurar la vigencia y efectividad de los sistemas antivirus en operación
2	Los usuarios no deberán instalar ningún antivirus diferente al dispuesto por la institución	Se recomienda que la alta dirección dé la directiva correspondiente para indicar la imposibilidad de instalar software por cuenta propia.

3	Los proveedores de los antivirus brindaran el soporte adecuado en el caso que se presente la necesidad para tal	Monitorear el desempeño de los servidores y de las maquinas de los usuarios para detectar situaciones no previstas por el proveedor de tal manera que se contrarreste la situación presentada.

Cuadro N °13: Virus informático

A continuación se muestra los diferentes tipos documentos que se utilizan a nivel de la unidad de informática (Cuadro N °14)

Nro	Documentos	Actividad	Responsable	Num. Copias
1	Memorando	Comunicar e informar a: Alta dirección, direcciones y/o jefaturas y unidades operativas del IMARPE	Jefe de la Unidad de Informática	Necesarias
2	Oficios	Comunicarse con Entidades externas (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación y ministerios)	Jefe de la Unidad de Informática	Necesarias
3	Correo Electrónico	Intercambio de información con entidades externas nacionales e internacionales (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación , ministerios y otros) y Alta dirección, direcciones y/o jefaturas y unidades operativas del IMARPE	Cada usuario que hace uso del servicio de correo	Necesarias
4	Informes	Informar a las entidades externas (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación , ministerios y otros) y Alta dirección, direcciones y/o jefaturas y unidades operativas del IMARPE, con Visto Bueno de la Alta Dirección	Jefe de la Unidad de Informática	Necesarias

Cuadro N °14: Documentos a nivel de la Unidad de Informática

4.1.1.3 Seguridad de Sistemas de Información

a) Ámbito de Aplicación

Este conjunto de políticas son aplicables al personal usuario de los sistemas de información institucionales.

b) Políticas

Las Políticas de seguridad de sistemas de información aplicables a los usuarios son:

De los Accesos a los Sistemas

Ítem	Política	Responsabilidad
1	Se establecerá un calendario para la modificación de passwords de acceso a los sistemas de información institucionales	Será responsabilidad de la Unidad de Informática coordinar con los responsables de los diversos sistemas o servicios para asegurar el cumplimiento de esta política
2	Mantener la privacidad de los datos e información administrados por los Sistemas Institucionales	Cada usuario es responsable del respectivo acceso autorizado
3	Las copias de respaldos de la información utilizada deberán salvaguardarse, desechando apropiadamente las no usadas. En el caso que se disponga darle de baja a algún equipo que contenga datos o información, se procederá a la destrucción previa de los contenidos	La Unidad de Informática es responsable de obtener las copias de respaldo de todos los sistemas bajo su administración. Toda unidad que administre datos deberá comunicarlo a la Unidad de Informática para incluirlo en sus procedimientos de copias de respaldo
4	Monitorear el estado de los servidores para verificar la fiabilidad de los contenidos	Los administradores de los servidores institucionales monitorearan y configuraran los servidores para asegurar la fiabilidad de los contenidos

Cuadro N °15: Accesos a los Sistemas de Información

De los Proveedores

Ítem	Política	Responsabilidad
1	Se establecerán cláusulas en los contratos con los proveedores que aseguren la privacidad y la propiedad del documento	La Unidad de Logística e Infraestructura , el Comité Especial de turno y la Oficina de Asesoría Legal en la revisión de los contratos para que los mismos cumplan con la política indicada.
2	Los proveedores solo pueden acceder a conjuntos de datos de muestra para la instalación de sus servicios	La Unidad de Informática en coordinación con los usuarios deberá proveer de los datos que permitan probar el sistema que se pondrá en producción. Para ello la unidad involucrada deberá reportar la presencia del proveedor en cuestión
3	Los proyectos de desarrollo que sean contratados deberán ser supervisados de tal manera que se garantice la recepción de los contenidos ofrecidos por los proveedores.	La Unidad de Informática es responsable de monitorear el cumplimiento de esta disposición siempre y cuando se le mantenga informada.

Cuadro N °16: Accesos a los Sistemas de Información

Nota. Se recomienda aplicar la "GUIA PARA LA ADMINISTRACION DE HARDWARE Y SOFTWARE" en aplicación a la Ley 28612 y su reglamento el D.S. 024-2006-PCM implementado en el IMARPE, cuando se requiera de nuevas adquisiciones de hardware y software.

A continuación se muestra los diferentes tipos documentos que se utilizan a nivel de la unidad de informática (Cuadro N °17)

Nro	Documentos	Actividad	Responsable	Num. Copias
1	Memorándum	TICs, Seguridad en la operatividad del sistemas IMARSIS	Jefe Informática	Necesarias
2	Guía de S&H.	Adquisición de hardware y software	DOA – UIeI, Comité de Adq. Con Asesoría de la UI	Necesarias
3	Cartilla de Instrucciones	Implementación de los sistemas de información	Jefe Informática	Necesarias
4	Correo Electrónico	Intercambio de información con entidades externas nacional e	Cada usuario que hace uso	Necesarias

		internacional (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación , ministerios y otros) y Alta dirección, direcciones y/o jefaturas y unidades operativas del IMARPE	del servicio de correo	
5	Informes	Informar a las entidades externas (proveedores, asociaciones, comunidad científica, empresas, institutos de investigación , ministerios y otros) y Alta dirección, direcciones y/o jefaturas y unidades operativas del IMARPE	Jefe de la Unidad de Informática	Necesarias
6	Acta de conformidad	Dar la conformidad de los servicios informáticos requeridos por el usuario con el apoyo de la Unidad de Informática.	Jefe de la Unidad de Informática y usuario	Necesarias
7	Plan de Gestión de la Seguridad de la Información	Implementación del plan de contingencia	Jefe de la UI y/o Subcomisión para tal	Necesarias
8	Manual técnico	Documentación técnica de los sistemas de información	Jefe de la Unidad de Informática	Necesarias

Cuadro N °17: Documentos de la seguridad de los sistemas de información

4.1.2 Revisión y Evaluación

Toda Política de Seguridad de la información debe ser revisada y evaluada. En la Institución se pueden dar cambios lo que implica una adecuación y alineamiento de la Política de Seguridad de la información que incluya los aspectos nuevos que hayan sido incorporados. Adicionalmente a ello la Política de Seguridad en marcha puede no ser efectiva en determinados aspectos, lo que también requiere de una modificación y adecuación. Finalmente la Política que este en aplicación debe ser dinámica para garantizar su efectividad.

Por lo anterior se ha dispuesto que la Unidad de Informática efectué el monitoreo del caso de manera periódica y proponga a la alta dirección los cambios que se consideren pertinentes.

Las acciones de intervención se deberán realizar ante sucesos no previstos y por tanto no estarán programadas. Como complemento de ello la Política de Seguridad de la información será revisada y evaluada periódicamente. Cada revisión se registrara de manera adecuada. Será obligatorio llevar un histórico de los cambios que se hayan producido.

Los aspectos que se deberán tener en cuenta en la mencionada evaluación son:

- Posibles efectos por cambios en los procedimientos, equipos, software, etc. Que pudieran afectar a la política de seguridad de la información y sus controles.
- La efectividad de la misma.
- Su costo de aplicación de la misma así como el costo de los controles asociados.

La alta dirección dispondrá e informará a toda la institución de la responsabilidad que asume la Unidad de Informática para evaluar la política de seguridad de la información.

Versión	Fecha	Descripción	Responsable	Apartados modificados
		Revisar y evaluar los procedimientos de respaldo de seguridad de los Sistemas Informáticos.	Jefe Informática	Todo el procedimiento

Cuadro N °18: Versión del Plan de seguridad de la información

5. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

5.1 Organización Interna

OBJETIVO: Administrar la seguridad de la información dentro del IMARPE y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del IMARPE.

5.1.1 Comité de gestión de seguridad de la información

5.1.1.1. Función del Comité de seguridad de la información propuesta

Dado el volumen de operaciones y la criticidad que presenta la información para el IMARPE y tomando en cuenta las mejores prácticas organizacionales, es necesaria la existencia de un Comité de coordinación de la información que administre la seguridad informática. Como requisito indispensable, esta función debe ser independiente de la Unidad de Informática, la cual en muchos casos es la ejecutora de las normas y medidas de seguridad elaboradas.

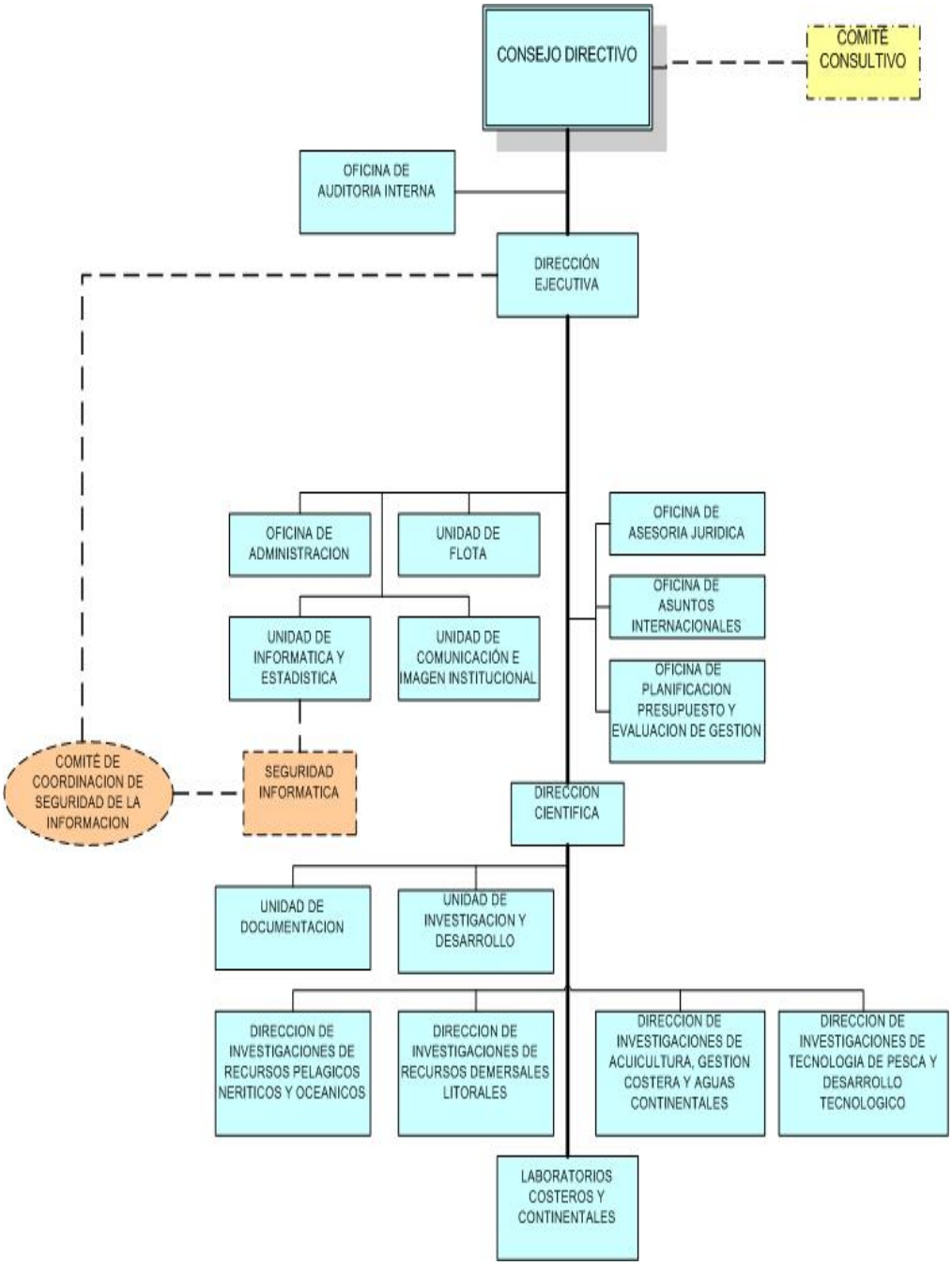

Figura 1: Estructura Organizacional Funcional propuesta para la administración de seguridad de la información

Considerando la falta de recursos con el perfil requerido que puedan ser rápidamente reasignados, el proceso de entendimiento y asimilación de las responsabilidades, los roles definidos correspondientes a la función de seguridad de informática, y la necesidad de implementar un esquema

adecuado de seguridad, se propone definir una Estructura Organizacional Funcional propuesta para la administración de seguridad de la información en la cual se creará un comité de coordinación de seguridad de la información para la definición de los objetivos y el monitoreo de las actividades de las mismas. Para mayor detalle. Ver. Figura 1

5.1.1.2. De la Conformación del Comité.

Es el equipo de personas que supervisa la implementación del Plan de Seguridad de la información, monitorea, propone y ejecuta los cambios requeridos al Plan de Seguridad de la información, por ello evalúa también la Política de Seguridad de la información.
Dicho comité deberá tener el respaldo de la Alta Dirección, ello permitirá una gestión efectiva y el respaldo correspondiente.

El Comité de Coordinación de la Seguridad de la Información estará conformado por:

- El Director Ejecutivo del Instituto del Mar del Perú – IMARPE.
- El Director Científico del Instituto del Mar del Perú – IMARPE.
- El Director de la Oficina de Administración del Instituto del Mar del Perú – IMARPE
- El Jefe de la Unidad de Informática del Instituto del Mar del Perú – IMARPE.
- Otros integrantes que el Director Ejecutivo considere pertinente incluir.

Para mayor detalle. Ver figura 2

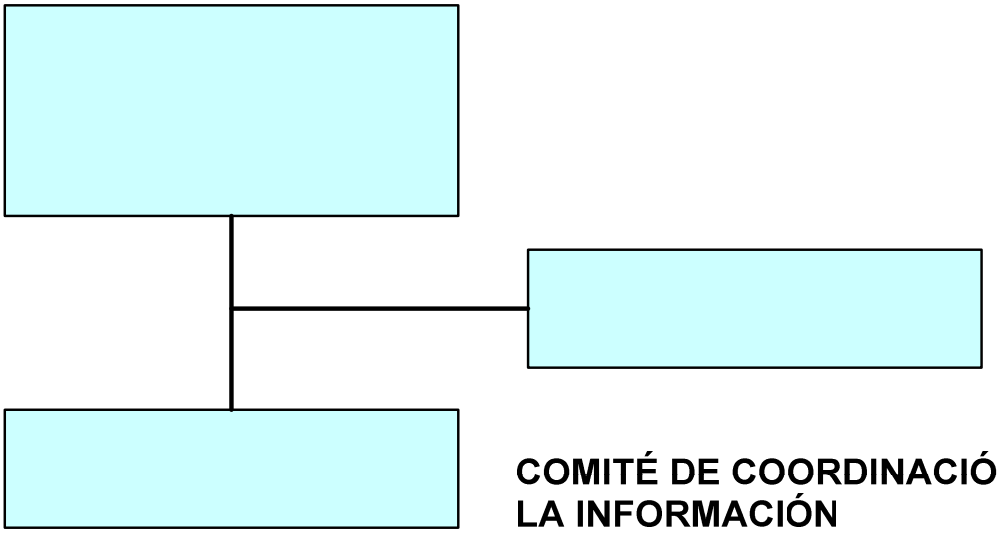

Figura 2: Organización del comité de coordinación de seguridad de la información.

5.1.1.3 De las Responsabilidades del Comité

Son responsabilidades del comité.

- Aprobar el Plan

  La definición del presente Plan de la Seguridad de la Información ha elaborado la Unidad de Informática y complementado por la Comisión designada mediante la R.D DE-046-2009. Esta Comisión lo eleva a la Dirección Ejecutiva para su revisión y modificación si fuera el caso.

- Disponer la Difusión del Plan

  El presente Plan, una vez aprobado debe difundirse y respaldarse por la alta dirección para garantizar su cumplimiento. Se determinara el mecanismo para asegurar el conocimiento del mismo por parte de todos los integrantes de la Institución.

- Disponer el cumplimiento del mencionado Plan.

  Indicar con claridad que es de cumplimiento obligatorio, especificando que existen sanciones ante su inobservancia.

- Monitorear y evaluar el cumplimiento del Plan.

  Establecer las sanciones y la aplicación de las mismas ante el incumplimiento del Plan. La Unidad de Informática establecerá un plan de monitoreo aleatorio que permita verificar el cumplimiento del Plan.

  Todos los usuarios del IMARPE poseen diversos servicios y accesos a los sistemas, datos e información de la Institución. Para poder determinar la Estructura Organizativa previamente se han definido roles.

  Llamamos rol a una función o papel que cumple un usuario Institucional. Es posible que un rol sea asumido por más de un usuario.

5.1.1.4 De los Roles

Denominamos rol a las funciones que una o mas personas pueden asumir en la administración de la información. Dado ello el rol debe poseer responsabilidades. Al implantar el Sistema de Gestión de la Seguridad de la Información se determinaran a las personas que participan en él, para ello se les asigna un rol.

Los roles previstos por el presente Plan son:

- Comité: Es el encargado de aprobar las políticas y los cambios del presente Plan. Dispone el cumplimiento y monitoreo de la aplicación del Plan aprobado.

Responsabilidad

El comité es el responsable de aprobar las políticas garantizando su cumplimiento mediante el monitoreo de la misma. El trabajo será desarrollado en coordinación con la Unidad de Informática.

- Comité: Conformado por personal que se dedica a la investigación o evaluación de los recursos y a la administración de bienes y servicios. Las personas de este rol administran series de tiempo referidas a sus labores diarias tanto en lo científico y administrativo.

Responsabilidad

Garantizar la seguridad de la información que esté bajo su responsabilidad. Cada científico que acceda a información o datos

institucionales coordinará con la Unidad de Informática para facilitar la administración de los contenidos.

- Administrador de Servidor: Es el encargado de monitorear los accesos a los servidores. Garantiza la salvaguarda de los contenidos de los mismos. Se deberán determinar con claridad los responsables de cada uno de los servidores institucionales lo que debe ser registrado.

Responsabilidad

La Unidad de Informática deberá monitorear la administración de los servidores para asegurar el cumplimiento de la norma.

- Administrativo: Personal que lleva a cabo labores para asegurar las operaciones de las diversas unidades de la Institución. Manejan la información y los datos asociados a dichas actividades.

Responsabilidad

La Unidad de Informática en coordinación con las unidades o direcciones administrativas monitoreará la administración de los datos e información Institucionales.

- Vigilante: Persona que controla el flujo de los que ingresen y salgan de la Institución.

Responsabilidad

La Unidad de Logística monitoreará las actividades de los vigilantes para asegurar el cumplimiento de su rol. La misma evaluará los mecanismos de control para su adecuación si fuese necesario.

5.1.2 Coordinación y responsabilidades de la seguridad de la información

Las políticas y procedimientos a implementarse deberían ser:

5.1.2.1 Coordinaciones

a) Establecer un coordinador de informática dentro de cada unidad operativa (coordinador usuario) con las funciones siguientes:

- Coordinar con la unidad de Informática, para solicitar acceso a la red, aplicaciones, etc.

- Coordinar todo lo relacionado al backup y restore con la Unidad de Informática.

b) Establecer normas sobre adquisición, desarrollo de aplicaciones, recuperación de datos y otras tareas complementarias aplicables a las PCs, asesorado por un profesional de informática o sistemas de la Unidad de Informática.

c) El uso de los recursos informáticos de la Institución (Hardware, software y datos) en los domicilios, procederá con autorización de la Alta Dirección

d) Controlar el movimiento de los recursos informáticos dentro y entre propiedades de la institución, como son: la Sede Central, Av. Argentina, Laboratorios costeros y los buques de investigación científica.

e) Conservar ocultos los discos flexibles y cartuchos, preferentemente bajo llaves, tanto en horas laborales como después de estos.

f) Prohibir el copiado de software, documentación y otros datos, sin autorización.

g) El inventario físico de hardware, equipos de computo, periféricos y equipos de comunicación debe estar actualizado

h) La Unidad de Informática coordinará con la Unidad de Logística e Infraestructura para planificar y ejecutar un plan de mantenimiento preventivo y correctivo de los equipos de cómputo, periféricos y equipos de comunicación.

- La encargada de la ejecución del plan será la Unidad de Logística e Infraestructura (Oficina de Mantenimiento) con el apoyo técnico de un profesional de sistemas de la Unidad de Informática
- En caso de que la oficina de mantenimiento no pueda realizar el servicio, se contrataría a un tercero

i) Mantener permanente contacto con todas las dependencias de la administración pública en el ámbito de la PCM – ONGEI establecido en su MOF según Decreto Supremo N° 094-2005-PCM Art. 37.

5.1.2.2 Responsabilidades

1) Instalar en el equipo un buen software antivirus dispuesto por la institución, con vacunas residentes en la memoria RAM y actualizarlo periódicamente en forma obligatoria.
2) Evitar o restringir el intercambio de dispositivos de almacenamiento de origen desconocido como: CD, DVD o Memoria USB, previa revisión por el antivirus instalado en una computadora personal.
3) Es muy importante que el antivirus elegido cuente además con un buen soporte técnico local.
4) Restringir al máximo el uso de los equipos, por parte de personas ajenas a las actividades propias de una entidad o dependencia.
5) Contar con una copia de respaldo en disquete, CD, DVD del sistema "buteable" y libre de virus, que además de los archivos ocultos, el COMMAND.COM y CONFIG.SYS incluya el SYS.COM para transferir el sistema en caso de borrarse o alterarse los archivos de sistema del disco. Es obligatorio que este disco de arranque tenga la misma versión del DOS o dispositivos de arranque. usada en el disco duro, o un disquete de Inicio si se usa Windows 98, Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows NT como sistema operativo.
6) En el caso de redes se deberá contar obligatoriamente con una copia de respaldo de los archivos que cargan la red.
7) Guardar copias de respaldo de los programas y archivos principales.
8) Los disquetes originales y las copias de respaldo deberán tener cerrado el seguro de protección contra escritura.
9) Mantener operativo los sistemas tape-backup para la prevención de pérdidas de información o simplemente como una cómoda opción de almacenamiento.
10) Los sistemas operativos Windows Vista, Windows XP, Windows 2000, Windows 98, Windows NT u otras versiones últimas, etc. son vulnerables a los virus. El hecho de que existen un buen número de

especies virales para ellos, se debe a que la cantidad de equipos que usan estas plataformas todavía son predominantes. Los autores de virus desean hacer daños masivos.

Cualquier medida preventiva para evitar los virus es buena aún cuando no sea la más adecuada

5.1.2.3 Registros de auditorias

Un rastro de auditoria o un registro cronológico completo (LOG) de transacción, puede ser una medida efectiva de seguridad. Es muy difícil construir un Sistema en el cual sea necesario que la seguridad sea proporcionada haciendo el sistema muy difícil de penetrar.

La forma más económica de conseguir la seguridad es hacer el sistema razonablemente difícil y además, proveerlo de rastros de auditoria y medios de detección para ubicar cualquier infiltración fructuosa. Tal detección debe entonces resultar en una acción disciplinaria.

Es altamente deseable que el sistema sea usado para elaborar la transacción de registros cronológicos (LOG) a fin de ver el potencial de violación de seguridad. Siendo necesario completarlo con un Sistema de Manejo Transaccional y de Intercambio de archivo (cuando esté a punto de llenarse el archivo inicial de LOG, o por motivos de necesidad de examinarlos), posibilitando el análisis y examen manual si fuera el caso.

La omisión de un Sistema de manejo por transacciones del registro cronológico (LOG), puede anular su uso como medida de seguridad. Actualmente los sistemas que están en producción no cuentan con un nivel de registro de auditoria, esto se puede implementar en los módulos desarrollados por IMARPE

Actualmente IMARPE esta desarrollando un proyecto de desarrollo e implantación de un sistema llamado IMARSIS. Este sistema está diseñado para llevar registros de auditorias.

5.1.3 Asignación de Responsabilidades Sobre Seguridad de la Información

Es importante mencionar que las responsabilidades referente a la seguridad de la información son distribuidas dentro de toda la organización y no son de entera responsabilidad del área de seguridad informática, en ese sentido existen roles adicionales que recaen en los propietarios de la información, los custodios de la información y el área de auditoria interna.

Los propietarios de la información deben verificar la integridad de su información y velar por que se mantenga la disponibilidad y confiabilidad de la misma.

Los custodios de la información tienen la responsabilidad de monitorear el cumplimiento de las actividades encargadas y el área de auditoria interna debe monitorear el cumplimiento de la política de seguridad y el cumplimiento adecuado de los procesos definidos para mantener la seguridad de la información. Los casos específicos están descritos en el apartado 5.1.2

Formato: Responsabilidad de Seguridad de la Información

El…….. (Director Ejecutivo del IMARPE), asigna las funciones relativas a la Seguridad Informática del IMARPE a .....(indicar cargo), en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del IMARPE, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo.

A continuación se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsable
Seguridad del Personal	DOA-UP
Seguridad Física y Ambiental	DOA-Todo el personal
Seguridad en las Comunicaciones y las Operaciones	DOA-UI
Control de Accesos a los usuarios	UI- Soporte Técnico
Seguridad en el Desarrollo y Mantenimiento de Sistemas	UI-Desarrollo
Planificación de la Continuidad Operativa	DOA-OPP-UI

Cuadro N °19: Responsable de los procesos de seguridad

De igual forma, seguidamente se detallan los propietarios de la información, quienes serán los Responsables de las Unidades Organizativas a cargo del manejo de la misma:

Información	Propietario	Recursos asociados	Procesos involucrados	Administrador
Contable	Jefe de Unidad de Contabilidad	Sistemas de información, equipamiento, bases de datos, comunicaciones	Contabilidad y presupuesto	DBA –Soporte técnico
Presupuesto	Jefe OPP	Sistemas de información, equipamiento, bases de datos, comunicaciones	Presupuesto	DBA –Soporte técnico
Inventario	Área de Patrimonio	Sistemas de información, equipamiento, bases de datos, comunicaciones	Inventario	DBA –Soporte técnico
Científica	Direcciones de Investigaciones	Sistemas de información, equipamiento, bases de datos, comunicaciones	Actividades de Investigación Científica	DBA –Soporte técnico

Cuadro N °20: Propietarios de la información

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

5.1.4 Proceso de autorización de recursos para el tratamiento de información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del IMARPE.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad Informática y deberá ser autorizado por el Responsable del Área Informática y por el Director Ejecutivo.

5.1.5 Acuerdos de confidencialidad

Confidencialidad o acuerdos de no divulgación deben anexar los requerimientos para proteger información confidencial usando términos ejecutables legales. Para identificar requerimientos de confidencialidad o acuerdos de no divulgación, se deben considerar los siguientes elementos:

a) Una definición de la información a ser protegida;
b) Duración esperada del acuerdo, incluyendo casos donde la confidencialidad pueda necesitar ser mantenida indefinidamente;
c) Acciones requeridas cuando un acuerdo sea finalizado:

d) Responsabilidades y acciones de los signatarios para evitar acceso desautorizado a la información

e) Propiedad de la información, secretos del comercio y de la propiedad intelectual, y como esto relaciona con la protección de la información confidencial;

f) La permisión de utilizar información confidencial y los derechos signatarios para usar la información

g) El derecho de auditar y monitorear actividades que impliquen información confidencial

h) Procesos para notificar y reportar acceso desautorizado a aberturas de información confidencial

i) Términos para que la información sea retornada o destruida en la cesación del acuerdo

j) Acciones prevista que se tomara en caso de una abertura de este acuerdo basados en los requerimientos de la seguridad de una organización, otros elementos pueden ser necesarios en un acuerdo de confidencialidad o de no-acceso.

Los acuerdos de confidencialidad y de no-acceso deben conformarse con todas las leyes aplicables y las regulaciones para la jurisdicción a la cual aplica (ver inciso 14.1.1)

Los requerimientos para acuerdos de confidencialidad y de no-acceso deben ser revisados periódicamente y cuando ocurran cambios que influyan en estos requerimientos.

5.1.6 Contacto con Autoridades

Dado a la cercanía al mar y estar ubicado en una zona de alto riesgo es que se mantiene en comunicación con instituciones que nos apoyaran en caso de ocurrir un desastre (ver siguiente cuadro)

Lista de Contacto de Autoridades			
Item	Organismos	Contacto	Teléfonos
01	INDECI	Coordinador de Defensa Civil Ing.	
02	EDELNOR		
03	TELEFONICA		
04	CLARO		
05	NEXTEL		
06	PRODUCE		
07	PCM-ONGEI		
08	CIA DE BOMBEROS		
09	SEDAPAL		
10	CAPITANIA DE PUERTOS		

Cuadro N °21: Listado de contacto de autoridades

5.1.7 Contacto con grupo de interés especial

Dado a que el IMARPE es una institución con implementación en el uso de tecnología de vanguardia en tema de seguridad es que se mantiene contacto con grupo de interés. (Ver cuadro adjunto)

Lista de Contacto con grupo de interés especial			
Item	**Organismo**	**Contacto**	**Teléfonos**
01	INICTEL-UNI		
02	ONGEI	Ing. Javier Panta	2744-356, 2744-358 : anexo 109

Cuadro N °22: Listado de contacto con grupo de interés especial

5.1.8 Revisión independiente de la seguridad de la información

La Unidad de Auditoria Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del IMARPE reflejan adecuadamente sus disposiciones.

5.2 Seguridad en los accesos de terceras partes

OBJETIVO: Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.

La seguridad de la información de la organización y las instalaciones de procesamiento de la información no deben ser reducidas por la introducción de un servicio o producto externo.

Debería controlarse el acceso a terceros a los dispositivos de tratamiento de información de la organización.

Cuando las actividades requieran dicho acceso de terceros, se debería realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deberían definirse y aceptarse en un contrato: con la tercera parte.

5.2.1 Identificación de riesgos por el acceso de terceros

Cuando exista la necesidad de otorgar acceso a terceras partes la información del IMARPE, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información del IMARPE.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro del IMARPE, se establecerán los controles, requerimientos de seguridad y compromisos de

confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

a) Personal de mantenimiento y soporte de hardware y software.

b) Limpieza, "catering", guardia de seguridad y otros servicios de soporte tercerizados.

c) Pasantías y otras designaciones de corto plazo.

d) Consultores.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

5.2.2. Requisitos de seguridad cuando se trata con usuarios externos

Todos los requisitos identificados de seguridad deben ser anexados a la seguridad antes de dar a los usuarios externos acceso a la información o a los activos del IMARPE. Para ello se tiene que aplicar los siguientes controles:

a) Protección de activos, que incluye lo siguiente:

1) Procedimientos para proteger los activos del IMARPE, incluida la información y el software

2) Procedimientos para determinar si ha ocurrido algún incremento del riesgo de los activos, por ejemplo una pérdida o modificación de datos

3) Medidas de integridad

4) Restricciones en la copia o divulgación de la información

b) La descripción del servicio o productos disponibles

c) Las diferentes razones, requerimientos y beneficios para el acceso del usuario externo

d) Acuerdos sobre control de accesos, donde se incluye lo siguiente:

1) Los métodos de acceso permitidos, así como el control y uso de identificadores únicos, como número de identificación ID y contraseñas.

2) El procedimiento de autorización del acceso y privilegios a los usuarios externos

3) Una declaración de que todo acceso que no esta explícitamente autorizado es prohibido

4) Un proceso para revocar el derecho de acceso o interrumpir la conexión entre sistemas

e) Arreglos para reportar, notificar e investigar inexactitudes de información (como detalles personales), incidentes y aberturas en la seguridad de información

f) Una descripción de cada servicio disponible

g) El nivel del servicio

h) El derecho para controlar y revocar cualquier actividad relacionado con los activos del IMARPE

i) Las respectivas responsabilidades del IMARPE y de los usuarios externos

Las respectivas responsabilidades en materia de legislación por ejemplo sobre protección de datos personales, teniendo especialmente en cuenta los diferentes sistemas legales nacionales si el contrato implica la cooperación con organizaciones de otros países (ver inciso 14.1)

j) Los derechos de propiedad intelectual, protección contra copias(ver inciso 14.1.2) y protección en tareas de colaboración (ver inciso 5.1.5)

5.2.3. Requisitos de seguridad en contratos con terceros (outsourcing)

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de seguridad de la información del IMARPE.

b) Protección de los activos del IMARPE, incluyendo:

- Procedimientos para proteger los bienes del IMARPE, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.

- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.

g) Existencia de Derechos de Propiedad Intelectual.

h) Definiciones relacionadas con la protección de datos.

i) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

n) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

o) Proceso claro y detallado de administración de cambios.

p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

r) Controles que garanticen la protección contra software malicioso.

s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

t) Relación entre proveedores y subcontratistas.

Los contratos acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC del IMARPE, contemplarán además de los puntos especificados en ("Requerimientos de Seguridad en Contratos o Acuerdos con Terceros"), los siguientes aspectos:

a) Forma en que se cumplirán los requisitos legales aplicables.

b) Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.

c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del IMARPE.

d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del IMARPE.

e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.

f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.

g) Derecho a la auditoria por parte del IMARPE sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc.

Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

6. CLASIFICACIÓN Y CONTROL DE ACTIVOS

6.1 Responsabilidad sobre los activos

OBJETIVO: Garantizar que los activos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

6.1.1 Inventario de activos

El IMARPE debe tener un conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, publicación científica, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos entre otros medios de almacenamiento), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es el área de patrimonio en coordinación con cada Responsable de Unidad Orgánica correspondiente.

Los inventarios de los activos ayudan a asegurar su protección eficaz, pero también se requiere para otros propósitos de la organización, por razones de prevención laboral, pólizas de seguros o gestión financiera.

6.1.1.1 Activos Identificados en el IMARPE

Los activos con que cuenta el IMARPE son:

- Equipos de computo y de comunicación

- Software en desarrollo y en producción
- Datos y bases de datos que son responsabilidad de informática
- Información producidas por las unidades operativas
- Oficinas

Equipos de cómputo y de comunicación

La lista de equipos debe ser revisada periódicamente para asegurar su permanente actualización. Inventario global de equipos y software del IMARPE que están bajo la responsabilidad de la Unidad de Informática son: Anexos 01, 02 y 04

Software en desarrollo y en producción

La lista de software que debe ser revisada periódicamente para asegurar su permanente actualización. Los softwares que están bajo la administración y/o responsabilidad de la Unidad de Informática. Ver anexo 03

Datos y Bases de Datos

Para cada software listado en el punto anterior existe una base de datos. Cada una de ellas está almacenada en los servidores de aplicaciones que administra la unidad de informática. Solo en el caso del software de planillas la base de datos correspondiente no se encuentra en ningún de los servidores dado que es una aplicación que corre localmente en la unidad de personal.

La Unidad de Informática es responsable tanto de cada una de las bases de datos en producción así como de las respectivas copias de respaldo. La misma unidad coordinara con la Unidad de Personal para aplicar el mecanismo de seguridad a la base de datos del sistema de planillas.

Oficinas

La Unidad de Informática cuenta con dos oficinas.

La oficina 307 o sala de servidores donde desarrollan sus actividades personal de soporte que son: Responsable del área de soporte, administrador de los servidores y Helpdesk.

La oficina 213 o despacho de la jefatura donde laboran 9 personas que son: La jefatura de la Unidad de Informática persona responsable de plantear o sugerir nuevas soluciones, secretaria de la Unidad de Informática, un administrador de la Web, un desarrollador Web, que se encarga de brindar mantenimiento a la Pagina Web del IMARPE, cuatros(04) desarrolladores de sistemas de información, que se encargar de desarrollar y brindar mantenimiento de sistemas de información y de un asesor que se encarga de apoyo a la jefatura de la Unidad de Informática, así como documentar y monitorear los proyectos del área de desarrollo de sistemas de información

6.1.2 Propiedad de los activos

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

Los propietarios de los activos deben ser responsables por:

- Asegurar que la información y los activos asociados con las instalaciones de procesamiento de información son apropiadamente clasificadas
- Definir y revisar periódicamente las restricciones de acceso y las clasificaciones, tomando en cuenta políticas de control aplicables.

La propiedad debe ser asignada a:

- Un conjunto definido de actividades
- Un conjunto definido de datos

6.1.3 Uso adecuado de los activos

Todos los empleados, contratistas y terceros deben de seguir las siguientes reglas o políticas para un uso aceptable de la información y de los activos asociados con las instalaciones del procesamiento de información, donde se incluye:

a) Mientras la administración del IMARPE tenga como objetivo proporcionar a un nivel razonable de privacidad de la red, los usuarios deben estar concientes que los datos que ellos crean y manipulan en los sistemas durante el desarrollo normal de sus actividades son propiedad y responsabilidad del IMARPE. Debido a la necesidad de proteger y vigilar la red y los sistemas del IMARPE, la administración no puede garantizar la confidencialidad absoluta de la información almacenada en cualquier dispositivo perteneciente al IMARPE.

b) Los usuarios del IMARPE deben tener criterio para decidir cuando pueden hacer uso personal de los recursos de tecnología de información y son los responsables de dichas decisión. De igual manera, los laboratorios costeros son los responsables de crear normas internas de uso personal de los servicios de Internet y de la red de IMARPE.

c) Para propósitos de mantenimiento de la red y de seguridad, las personas autorizadas dentro del IMARPE podrán monitorear equipos, sistemas y tráfico de red en cualquier momento, de acuerdo con la política de auditoria de sistemas para seguridad informática del IMARPE.

d) El IMARPE se reserva el derecho para auditar las redes y los sistemas periódicamente para garantizar el cumplimiento de esta política.

Usos inadecuados

Bajo ninguna circunstancia los miembros del IMARPE pueden utilizar los recursos del mismo, para realizar actividades prohibida por la normas de la institución o por normas jurídicas nacionales o internacionales.

La siguiente es una lista de actividades que, sin ser completa, intenta proporcionar una referencia de las actividades que se ajustan a la categoría de uso inadecuado para “sistemas y redes”, y para “correo electrónico y sistemas de comunicaciones”.

Actividades en los sistemas y en red

Las siguientes actividades están prohibidas:

1. Violaciones de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia de uso adecuado adquirido por IMARPE (software “pirata”).
2. Copia no autorizada de material protegido por derechos de autor que incluye, pero no esta limitado a, digitalización y distribución de imágenes o fotografías de cualquier origen(revistas, libros, paginas Web, etc.), digitalización y distribución de música, audio, o video, distribución e instalación de software de los cuales ni el IMARPE ni el usuario tienen la licencia debida.
3. Introducción de software malicioso en la red en los servidores (virus, gusanos, ráfagas de correo electrónico no solicitado, etc.).
4. Revelar la clave o código de su cuenta a otros (por ejemplo, su cuenta de correo electrónico, su usuario de base de datos, su código para realizar llamadas de larga distancia) o permitir sus uso a terceros para actividades ajenas a la misión del IMARPE. La prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario, empleados o practicantes del IMARPE cuando la actividad se realiza desde el hogar (por ejemplo, computadores portátiles, teléfonos celulares o agendas electrónicas propiedad del IMARPE).
5. Utilizar la infraestructura de tecnología de información del IMARPE para conseguir o transmitir material con ánimo de lucro. Igualmente se prohíbe el uso del sistema de comunicaciones del IMARPE con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.
6. Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios del IMARPE
7. Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios. Entre las acciones que

contravienen la seguridad de la red se encuentran, aunque no están limitadas es, acceder a datos cuyo destinatario no es usted, ingresar a una cuenta a un servidor o de una aplicación para la cual no esta autorizado. Para propósito de esta sección la palabra “interrupción” incluye, pero no esta limitada a, capturar trafico de la red, inundar de *pings* la red(*ping* es un comando que permite verificar que otro equipo esta activo para la red), realizar *spoofing* de paquetes(*spoofing* es la falsificación de la dirección de la red), ataques distribuidos de negación de servicios (agresiones desde la red buscan que servicios validos como correo electrónico o el servidor Web se “ocupen” y no atiendan a usuarios legítimos. Se conocen también como ataques DDoS) o falsificar información de enrutamiento y de configuración de los equipos y sistemas con el objetivo de aprovechar alguna vulnerabilidad.

8. Esta prohibido explícitamente el monitoreo de puertos o analiza de trafico de red con el propósito de evaluar vulnerabilidades de seguridad. Las personas responsables de la seguridad informática pueden realizar estas actividades cuando se realicen en coordinación con el personal responsable de los servidores, los servicios, las aplicaciones y de la red.
9. Ejecutar cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada.
10. Burlar los mecanismos de seguridad, autenticación, autorización o de auditoria de cualquier servicio de red, aplicación, servidor, o cuenta de usuario.
11. Interferir o negar el servicio a usuarios autorizados con el propósito de lesionar la prestación del servicio o la imagen del IMARPE (por ejemplo ataques DDoS)
12. Uso de comandos o programas o el envió de mensajes de cualquier tipo con el propósito de interferir os deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

Actividades con el correo electrónico y sistemas de comunicación

Las siguientes actividades están prohibidas:

1. Enviar mensajes de correo no solicitadas, incluyendo junk mail (material publicitario enviado por correo) o cualquier tipo de anuncio comercial a personas que nunca han solicitado ese tipo de material (email spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).
2. Cualquier forma de acoso a través de correo electrónico, teléfono o mensajes a localizadores personales (*beepers*) sin importar el idioma, la periodicidad o tamaño del mensaje.
3. Generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
4. Envió de mensajes de correo electrónico con una dirección de correo diferente al verdadero remitente con el fin de realizar algún tipo de acoso, difamación u obtener información
5. Crear o reenviar cartas cadena o cualquier otro esquema de "pirámide" de mensajes.
6. Colocar mensajes de correo iguales o similares no relacionados con las actividades del IMARPE a un gran número de grupos de noticias (newsgroup spam, mensajes, electrónicos masivo, no solicitados y no autorizados en grupos de noticias).

6.2 Clasificación de la Información

OBJETIVO: Asegurar un nivel de protección adecuado a los activos de información. La información debería clasificarse para indicar la necesidad, prioridades y grado de protección.

La información tiene grados variables de sensibilidad y criticidad. Algunos elementos de cada información pueden requerir un nivel adicional de protección o un uso especial. Debería utilizarse un sistema de clasificación de información para definir un conjunto de niveles de protección adecuados, y comunicar la necesidad de medidas de utilización especial.

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

- Confidencialidad:

  0 - Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del IMARPE o no. PUBLICO

  1 - Información que puede ser conocida y utilizada por todos los empleados del IMARPE y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el IMARPE, el Sector Público Nacional o terceros. RESERVADA – USO INTERNO

  2 - Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al IMARPE, al Sector Público Nacional o a terceros. RESERVADA – CONFIDENCIAL

  3 - Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del IMARPE, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

- Integridad:

  0 - Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del IMARPE o no. PUBLICO

  1 - Información que puede ser conocida y utilizada por todos los empleados del IMARPE y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el IMARPE, el Sector Público Nacional o terceros. RESERVADA – USO INTERNO

  2 - Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o

uso no autorizados podría ocasionar pérdidas significativas al IMARPE, al Sector Público Nacional o a terceros. RESERVADA – CONFIDENCIAL

3 - Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del IMARPE, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

- Disponibilidad:

  0 - Información cuya inaccesibilidad no afecta la operatoria del IMARPE.

  1 - Información cuya inaccesibilidad permanente durante (recomendable un plazo no menor a una semana) podría ocasionar pérdidas significativas para el IMARPE, el Sector Público Nacional o terceros.

  2 - Información cuya inaccesibilidad permanente durante (recomendable un plazo no menor a un día) podría ocasionar pérdidas significativas al IMARPE, al Sector Público Nacional o a terceros.

  3 - Información cuya inaccesibilidad permanente durante (recomendable un plazo no menor a una hora) podría ocasionar pérdidas significativas al IMARPE, al Sector Público Nacional o a terceros.

Al referirse las pérdidas, se contemplan aquellas mensurables (materiales) y no mensurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- CRITICIDAD BAJA: ninguno de los valores asignados superan el 1.
- CRITICIDAD MEDIA: alguno de los valores asignados es 2
- CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.

- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

En adelante se mencionará como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

6.3 Implementación de inventarios y clasificación de activos de Información

OBJETIVO: Realizar el inventario, clasificar y manejar información que generen, posean o utilicen información los funcionarios del IMARPE, llevando acabo las actividades que bajo su responsabilidad tendrán propietarios o custodios técnicos de los archivos de información.

6.3.1 Procedimiento de inventarios de activos de información

ID	(QUE) ACTIVIDAD	(QUIEN) RESPONSABLE	(COMO) TAREA	REGISTROS
1	Realizar levantamiento de información para inventario de activos de información	Comité de inventario de información	Diligenciar la matriz "DEFINICION DE ACTIVOS POR PROCESOS" medio magnético, etc.	Formato de levantamiento de información de activos. Ver. (Anexo 8)
2	Validar la información de los activos de información	Gestor de calidad Propietario del activo de información Custodio técnico de los activos de información	Revisión de la definición de activos realizadas por el propietario y del custodio técnico designado Registrar a la matriz definición de activos por proceso. Enviar mediante comunicación interna la definición de activos de información en medio magnético a la unidad de informática	Formato de levantamiento de información de activos. Ver. (Anexo 8) Comunicación Interna
3	Integrar la	Profesional	Integrar la información de las	Formato: Matriz

	información en la matriz de inventario y clasificación de activos	especialista en sistema de información	matrices "definición de activos por proceso" enviados por las diferentes direcciones, jefaturas y laboratorios costeros en la matriz de inventario y clasificación de activos.	de inventario y clasificación de activos de información. Ver. (Anexo 9)
4	Clasificar los activos de información	Profesional especialista en sistema de información	Asignar los niveles de clasificación de acuerdo con la información consignada en la matriz de inventario y clasificación de activos de la seguridad de la información	Formato: Matriz de inventario y clasificación de activos de información. Ver.(Anexo 9)
5	Publicar y divulgar el activo de información	Profesional especialista en sistema de información	Publicar en la Intranet el inventario de activos de información Realizar una presentación formal del documento de inventario y clasificación de activos de información como mínimo a las personas que aparezcan como propietarios o custodios técnicos de algún activo(no aplica para actualizaciones)	Formato: Matriz de inventario y clasificación de activos de información. Ver. (Anexo 9) Formato: registro de asistencia. Ver. (Anexo 10)
6	Revisar y actualizar la matriz de inventarios y la clasificación de activos	Gestor de calidad de cada dirección o laboratorio conjuntamente Profesional especialista en sistema de información	La matriz de inventario se revisa semestralmente o si se solicita por un gestor de calidad o la Unidad de Informática. Revisar la matriz de inventarios y clasificación de activos Determinar si los activos de información son para actualizar o definir nuevos. Ir al paso 2	N/A

Cuadro N °23: procedimiento de inventarios de activos de información

7. SEGURIDAD EN RECURSOS HUMANOS

7.1 Seguridad en la definición del trabajo y los recursos (Antes del empleo)

OBJETIVO: Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. La seguridad debería contemplarse desde las etapas de selección de personal, incluirse en los contratos y seguirse durante el desarrollo de la relación laboral. Deben filtrarse adecuadamente los candidatos (ver inciso 7.1.2), sobre todo para tareas sensibles. Todos los empleados y los terceros, usuarios de aplicaciones de tratamiento de información, deberían firmar una cláusula de confidencialidad (no divulgación).

7.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales

Las funciones y responsabilidades sobre la seguridad de la información, así como cualquier responsabilidad específica para la protección de activos y la ejecución de procesos están contempladas respectivamente en el Manual de Organización y Funciones – MOF para el trabajador permanente, y en los contratos respectivos amparados por el código civil para los trabajadores CAS. Ver Portal del IMARPE (transparencia): Manual de Organización y Funciones del IMARPE y modelo de contrato (Anexo 11).

7.1.2 Selección y política de personal

Cada nuevo empleado de la Organización es una apuesta de futuro. La Institución asigna una serie de tareas y responsabilidades al nuevo empleado, y le proporciona los medios materiales y la información necesaria para que pueda llevarlas a cabo. Debe existir un procedimiento de Selección y contratación del personal que tenga en cuenta los siguientes aspectos relativos a la seguridad:

a) Definición del puesto: Para cada nueva vacante se debe definir la criticidad del puesto a cubrir según su responsabilidad y la información que maneja. El IMARPE debe definir su criterio propio. Algunos puestos críticos pueden ser directivos, jefaturas, personal de seguridad, personal de contabilidad, etc.

b) Selección: En la selección de candidatos a puestos críticos se deben comprobar los antecedentes penales y las referencias profesionales.

c) Contrato: El contrato laboral debe incluir los correspondientes acuerdos de confidencialidad, propiedad intelectual y protección de datos.

d) Comienzo: Durante los primeros días de trabajo, es recomendable que el empleado:

- Asista a unas sesiones de formación donde se le introduzca en la normativa interna y de seguridad de la institución. De este modo todo empleado conoce sus obligaciones de seguridad tales como la protección de sus claves de acceso, uso adecuado del email e Internet, clasificación de la información, etc.
- Reciba el manual de normativa interna y firme el compromiso de cumplimiento del mismo. Este trámite establece formalmente las normas internas y garantiza que el empleado conoce la normativa existente.

e) Accesos: Los accesos a la información y sistemas informáticos deben ser solicitados siempre por el responsable directo del empleado a la Unidad de Informática donde el área de HelpDesk les atenderá. Dichos accesos deben ser siempre justificables por la labor que se va a realizar, y en caso de ser privilegiados, el Departamento de Seguridad debe aprobar su concesión.

Ver grafico 1: diagrama de selección y política de personal

Los directivos deberían conocer qué circunstancias privadas de su personal pueden afectar a su trabajo. Los problemas personales o financieros, los cambios de su comportamiento o estilo de vida, las ausencias recurrentes y la depresión o el estrés evidentes podrían llevar a fraudes, robos, errores u otras implicaciones de seguridad. Esta información debería manejarse de acuerdo con la legislación correspondiente.

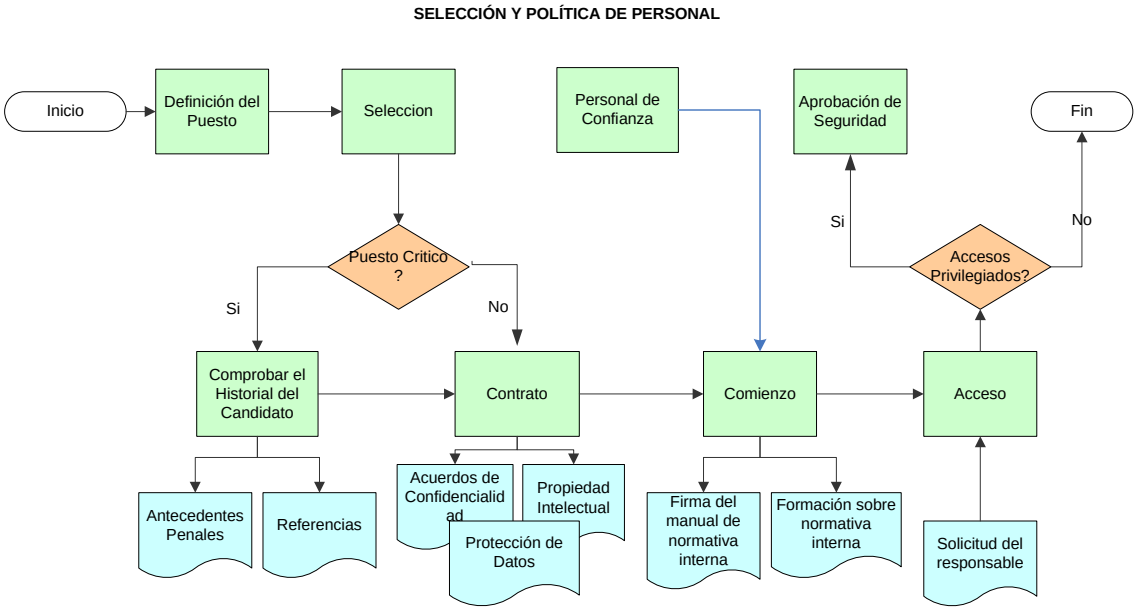

Grafico 1: Diagrama de Selección y Política de personal

7.1.3 Acuerdos de confidencialidad

Como parte de sus términos y condiciones iniciales de empleo, los empleados, revisarán la documentación y firmarán un *Compromiso de confidencialidad, aceptación de la Política de Seguridad de la Información y utilización de recursos informáticos*, en lo que respecta al tratamiento de la información del IMARPE. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra área competente.

Asimismo, mediante el *Compromiso de confidencialidad, aceptación de la Política de Seguridad de la Información y utilización de recursos informáticos* el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

MODELO: COMPROMISO DE ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CONFIDENCIALIDAD Y UTILIZACIÓN DE RECURSOS INFORMÁTICOS

El que suscribe, ... DNI ..... , declara conocer y aceptar todas las obligaciones emergentes de la Política de Seguridad de la Información adoptada por el IMARPE en la que desempeño mis funciones y que se adjuntan, así como también de todas las normas, procedimientos y prácticas que de ella surjan.

Mediante la suscripción del presente instrumento, me comprometo a usar la información adquirida en el ejercicio o con motivo del ejercicio de mis funciones solamente para el uso específico al que se la ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona física o jurídica o entidad, salvo en caso que la clasificación que le hubiese asignado el Propietario de la Información - entendiéndose por tal al funcionario al que se le hubiere asignado la responsabilidad de clasificar la información de su propiedad de acuerdo con el grado de sensibilidad y criticidad de la misma, documentar y mantener actualizada la clasificación efectuada - así lo permita o mediase su aprobación previa y por escrito, todo ello bajo exclusiva responsabilidad de quien suscribe.

Para el caso de ser necesario entregar información a terceras personas, me comprometo a verificar previamente que destinatario de la información y/o el organismo en el cual desempeña sus tareas, haya suscripto un compromiso o acuerdo de confidencialidad que lo obligue a no divulgar a terceros la información recibida, haciéndome responsable de los daños y perjuicios que pudiere ocasionar su difusión en caso de no tomar esta medida.

Considerando que los recursos de procesamiento de información del IMARPE se suministran con un propósito determinado, me comprometo a utilizar los que me fueran asignados para el desempeño de mis funciones de manera racional, evitando su abuso, derroche o desaprovechamiento, aceptando a tales fines que las actividades que realice sean objeto de permanente control y monitoreo.

La obligación de reserva o confidencialidad asumida en virtud del presente compromiso seguirá vigente después de finalizada la tarea encomendada y aún después de la rescisión o resolución del contrato o cese o interrupción de la relación de empleo que me vincula con la Administración Pública Nacional, por el

plazo de 5 (cinco) años, haciéndome responsable de los daños y perjuicios que pudiere ocasionar la difusión de datos o informes no publicados.

El presente compromiso de ninguna manera sustituye la normativa vigente aplicable a la función que desempeño.

Firma_____DNI o Carnet de Extranjería: _____

Cargo:_____Área:_____

Fecha: _____

Términos y condiciones de la relación laboral

La relación laboral con trabajadores estables:

- Los términos y condiciones de empleo; se desarrollan en lo ético al amparo de las normas que rige al empleado público.
- El desempeño de cada puesto o plaza exige requisitos claramente establecidos en el Portal del IMARPE (transparencia): Manual de Organización y Funciones del IMARPE.
- La ejecución de procedimientos están contempladas en el Manual de Procedimientos de cada Unidad Operativa de la Institución.

La relación laboral para trabajadores CAS, se rige en los términos y condiciones establecidas en las cláusulas del contrato. Manual de Procedimientos (en desarrollo) y el modelo de contrato (ver anexo 9).

7.2 Seguridad en recursos humanos (durante del empleo)

OBJETIVO: Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo. Los usuarios deberían recibir formación en procedimientos de seguridad y en el uso correcto de los recursos de tratamiento de información para minimizar los posibles riesgos en la seguridad.

7.2.1 Responsabilidad de la Alta Dirección

Las responsabilidades de la Alta Dirección deben incluir, asegurase de que los empleados, CAS y terceros:

a) Contar con un resumen apropiado de sus responsabilidades y roles en la seguridad de información antes de garantizar el acceso a información sensible o a los sistemas de información.

b) Estar provistos con una guía que establezca las expectativas de seguridad de su rol dentro del IMARPE.

c) Que se encuentren motivados de cumplir las políticas de seguridad del IMARPE.

d) Alcancen un nivel de conocimiento de seguridad relevante en sus roles y responsabilidades dentro del IMARPE

d) Que estén conforme con los términos y condiciones del empleo, los cuales incluyen la política de seguridad de la información y métodos apropiados de trabajo

f) Continúen teniendo habilidades y calificaciones apropiadas

7.2.2 Formación y capacitación en seguridad de la información

Todos los empleados del IMARPE y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el IMARPE, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del IMARPE. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Es recomendable que cada 3 meses se revise el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de producir el material de capacitación (ver cuadro N °24)

Nro	Áreas Responsables del Material de Capacitación
1	DOA - Recursos Humanos
2	OPP

Cuadro N °24: Áreas responsables de capacitación

El personal que ingrese al IMARPE recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se evaluaran los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

Los usuarios (nivel directivo, profesional, técnico, etc.) que necesiten de cualquier apoyo en seguridad en software de uso oficial, deben de comunicarse con la Unidad de Informática con la finalidad de obtener atención en requerimientos que consisten: En instalación y configuración de software básico o especializado y administración de los mismos. Anexo 3.

7.2.3 Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales directivos apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se

encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Sin perjuicio de informar a otros Organismos de competencia, el Responsable de Seguridad Informática, comunicará al Comité de Contingencia y Seguridad todo incidente o violación de la seguridad, que involucre recursos informáticos.

Todos los empleados y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

7.2.4 Proceso disciplinario

El proceso disciplinario no debe comenzar sin una verificación previa de que la apertura en la seguridad ha ocurrido.

El proceso formal disciplinario debe asegurar un correcto y justo tratamiento de los empleados que son sospechosos de cometer aperturas en la seguridad. El proceso formal disciplinario debe proveer de una respuesta graduada que tome en consideración factores como la naturaleza, la gravedad de la apertura y su impacto de las actividades, si es que la falta es repetida o única o si es que el violador estuvo propiamente entrenado, leyes relevantes, contratos de negocios así como otros factores si son requeridos. En casos serios de mala conducta el proceso debe permitir el retiro de sus labores, derechos de acceso y privilegios así como una escolta inmediata fuera del sitio, si es que necesario.

7.3 Finalización o cambio del empleo

OBJETIVO: Asegurar que los empleados, contratistas o usuarios terceros salgan de la organización o cambien de empleo en una forma ordenada.

Las responsabilidades se establecen con el fin de asegurarse que la salida de la organización de los empleados, contratistas o usuarios terceros está manejada y que el retorno de todo el equipo y el retiro de todo derecho de acceso a los sistemas.

Cambios en la responsabilidad y empleos dentro de la organización deben ser manejados como la terminación de la respectiva responsabilidad o empleo, en línea con esta sección y cualquier nuevo empleo debe ser manejado como se describió en la sección 7.1

7.3.1 Responsabilidad de finalización

La salida de un empleado es un punto crítico de riesgo para la Organización. En casos de problemas laborales y despidos, un empleado modelo hasta la fecha, puede convertirse en una seria amenaza. La historia reciente está plagada de casos de sabotaje o substracción de información por parte de empleados "disgustados".

Lamentablemente, es bastante común que no se gestionen coordinadamente las bajas de los empleados. En muchas ocasiones, Recursos Humanos se encarga de realizar los trámites legales de la baja, mientras que el responsable del empleado es quien trata directamente con él y planifica el traspaso de su trabajo. Por otro lado, la Unidad de Informática se ocupa de dar de baja sus accesos (en el momento en que comuniquen su ausencia). Este escenario acaba degenerando en problemas tales como que los accesos de los ex empleados siguen vigentes durante meses, o que tras la marcha del empleado no es posible recuperar cierta información vital que poseía. Para evitar todo esto, debe existir un procedimiento de bajas que tenga en cuenta los siguientes aspectos de seguridad:

a) Clasificación de las bajas: El responsable del empleado vía Recursos Humanos deben clasificar la baja según las circunstancias que la rodean. Un ejemplo de posibles categorías sería:

- Baja normal, si se produce en circunstancias normales y sin conflictos.
- Baja cautelar, si se produce en circunstancias normales, pero con la que hay que tener una vigilancia especial en los accesos y documentación que obra en poder del empleado: personal con acceso a información sensible, administradores de sistemas, etc.
- Baja crítica si se produce en circunstancias especiales: despidos, problemas con el empleado, etc.

b) Comunicación de las bajas: Tan pronto se conozca la baja de un empleado, Recursos Humanos debe comunicar las bajas de personal a Seguridad. En la comunicación se debe indicar el nombre, la fecha efectiva de la baja, su clasificación y cualquier medida o control especial que sea necesario realizar.

c) Gestión de las bajas: Seguridad debe coordinar que la baja se produzca en el plazo adecuado dependiendo de la clasificación (por ejemplo, una baja crítica debe realizarse de forma inmediata). Debe efectuarse la retirada de:

- accesos físicos (llaves, cajas fuertes, llaves electrónicas)
- accesos lógicos (email, acceso a la red y servidores, etc.)
- material de la empresa (portátil, móvil, etc.)

La gestión de la baja también puede incluir otras medidas dependiendo de la clasificación de la misma:

- realización de copias de seguridad de la información sensible
- Supervisión de los accesos hasta el día de la baja
- Cancelación preventiva de los accesos más críticos

Ver grafico 2: Diagrama de salida de empleados

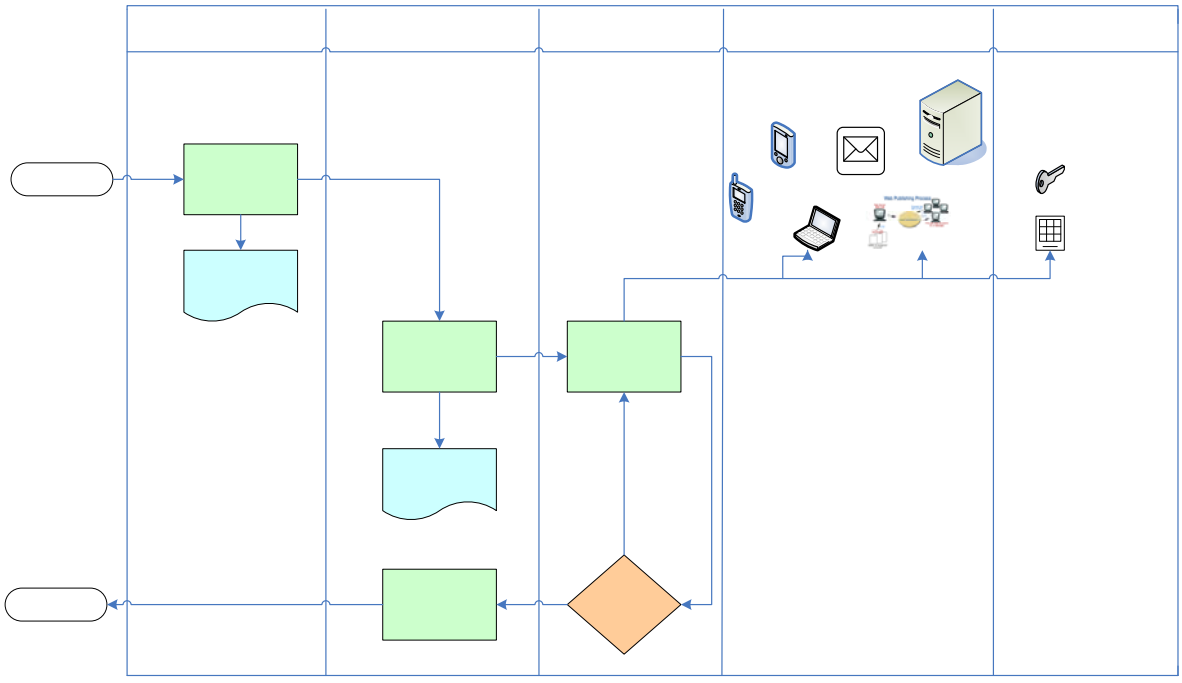

Grafico 2: Diagrama de Salida de Empleados

7.3.2 Retorno de activos

El proceso de finalización debe ser formalizado mediante un documento (memorando, correo electrónico) para que entregue los activos como: software,

documentos corporativos y equipos. Otros activos de la organización como dispositivos móviles de cómputo, tarjetas de crédito, tarjetas de acceso, manuales, software e información guardada en medios electrónicos, también necesitan ser devueltos. Los activos deben ser recepcionados por su jefe inmediato superior.

En caso donde el empleado, CAS o tercero compra el equipo de la organización o usa su propio equipo, se debe seguir procedimientos para asegurar que toda la información relevante es transferida a la organización y borrado con seguridad del equipo (véase el inciso 9.7.1)

En casos donde un empleado, CAS o tercero tiene conocimiento que es importante para las operaciones en curso, esa información debe ser documentada y transferida a la organización.

7.3.3 Retiro de los derechos de acceso

Hasta la culminación, se debe reconsiderar los derechos de acceso de un individuo a los activos asociados con los sistemas de información y a los servicios. Esto determinara si es necesario retirar los derechos de accesos. Los cambios de un empleo deben ser reflejados en el retiro de todos los derechos de acceso que no fueron aprobados para el nuevo empleo. Los derechos de acceso deben ser removidos o adaptados, incluyendo acceso físico y lógico, llaves, tarjetas de identificación, instalaciones del proceso de información (véase el inciso 10.2.4), subscripciones y retiro de cualquier documentación que los identifica como un miembro actual de la organización. Si un empleado, CAS o usuario de tercero saliente ha sabido contraseñas para activos restantes de las cuentas, deben ser cambiadas hasta la finalización o cambio del empleo, contrato o acuerdo.

Los derechos de acceso para activos de información y equipos deben ser reducidos o removidos antes que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo como:

a) Si la finalización o cambio es iniciado por el empleado, CAS o usuario de tercero, o por la dirección y la razón de la finalización
b) Las responsabilidades actuales del empleado u otro usuario.
c) El valor de los activos a los que se accede actualmente

8. SEGURIDAD FÍSICA Y DEL ENTORNO

8.1 Áreas seguras

OBJETIVO: Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes: Central, Av. Argentina, BICs y Laboratorios de Investigación descentralizados e información del IMARPE.

Proteger el equipamiento de procesamiento de información crítica del IMARPE ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del IMARPE.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

8.1.1 Perímetro de seguridad física

EN LA SEDE CENTRAL

La protección física del IMARPE en la comprensión de la Av, Gamarra y Gral. Valle, esta constituido por el cerco perimétrico y enrejados hasta el acceso al muelle.

Dos portones de entrada por la Av. Gamarra, una puerta de entrada para personal que labora en la institución y visitantes por la calle Gral. Valle y un portón de entrada al muelle de embarque y desembarque. Además; la presencia permanente de servicio de vigilancia.

EN EL LOCAL DE LA AV. ARGENTINA

Su ubicación está en una zona industrial que de por si está cercado por los lados norte, este y oeste.

El lado sur está constituido por un portón para acceso de vehículos y una puerta de entrada que es ubicación de un (1) vigilantes durante las 24 horas del día, con funciones de ejercer control del personal que labora en dicho local

o visitantes que proceden de la sede central del IMARPE por motivos de investigación o logística, así como la visita de público en general.

EN EL LOCAL DE LOS LABORATORIOS DE INVESTIGACION DESCENTRALIZADOS

Con diferencias menores, el local de cada uno tiene el perímetro cercado con un portón de entrada que es la ubicación de dos vigilantes durante las 24 horas del día.

Los vigilantes están encargados del control de las salidas y entradas del personal que labora en ella como de los visitantes, así como de los equipos mediante un documento de control.

Existe la necesidad de incrementar el número de vigilantes por el incremento de equipos sofisticados debido a la especialización de los respectivos laboratorios.

EN LOS BICs Y EMBARCACIONES MENORES

La seguridad física en los BICs OLAYA, HUMBOLDT y EMBARCACIONES MENORES, está constituido por tres (3), cinco (5) y un (1) personal de guardia respectivamente provistos de comunicación radial con la sede central, con misión de realizar guardia durante las 24 horas.

Cuando los BICs no están navegando (Cruceros) generalmente se encuentran ancladas aproximadamente a una distancia de ½ milla totalmente dispuestos de hacerse a la mar en caso de tsunami u otra urgencia de carácter emergencia.

8.1.2 Controles físicos de entradas

La protección de seguridad en la entrada se rige por los siguientes controles:

- Identificación, registro, supervisión de control electrónico de asistencia en la entrada y salida al personal que labora en la institución.
- Identificación, registro de entrada y salida del personal visitante, así como la identificación de la persona o Unidad operativa visitada.

- Registro de salidas y entradas por motivos de comisión de trabajo u otros dentro del horario de la jornada laboral.
- Registro de salida y entrada de todo bien perteneciente al IMARPE por motivo de reparación, préstamo u otras causas.
- Registro de salidas y entradas de vehículos al servicio de IMARPE en las otras puerta a cargo del servicio de vigilancia.

8.1.2.1 Controles físicos de equipos de cómputo

Estos controles son seleccionados adecuadamente para microcomputadoras y debe incluir también la consideración de factores tales como los efectos del calor, el aire acondicionado y la humedad sobre los microcomputadores frente a las fluctuaciones o picos de tensión eléctrica.

Un plan que asegure un ambiente físico favorable y seguro para la institución debería hacer lo siguiente:

a) Establecer procedimientos que aseguren el control de aquellos equipos en préstamos cuando no sean devueltos en un período de tiempo especificado.

b) Notificar al responsable del inventario y a la Unidad de Informática y Estadística los recursos cedidos o prestados a terceros.

c) Alertar al personal adecuado sobre la existencia de condiciones que contribuyan a generar electricidad estática.

d) Exigir un documento formal en aquellos casos en que se produzca cambio en la custodia de hardware o software dentro o fuera del local del IMARPE, incluyendo la firma de las partes implicadas e informar a la Unidad de Informática y Estadística.

e) Controlar el movimiento entre oficinas e instalaciones de los equipos de microcomputador e informar a la Unidad de Informática y Estadística.

f) Identificar todo el hardware con etiquetas de seguridad que no se puedan desprender fácilmente y que resulten fácilmente legibles para permitir la identificación en caso de substracción.

g) Considerar el uso de dispositivos de seguridad física que hagan difícil el traslado de los equipos.

h) Implantar un procedimiento de control de acceso al área de sistemas donde se encuentran los servidores y los backup de seguridad.

i) Comunicar inmediatamente a la Unidad de Informática y Estadística sobre la presencia de virus informáticos vía Internet u otros medios.

j) Cuando los usuarios requieren la instalación y configuración de software deben de comunicar a la Unidad de Informática y Estadística.

k) En todos los servidores y estaciones de trabajos y especialmente los servidores deben tener instalado un software antivirus.

8.1.3 Seguridad de oficinas, despachos y recursos

En relación a la Sala de Servidores

a) Es recomendable que la sala de Servidores no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.

b) Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad de la Sala de Servidores.

c) El acceso a la Sala de Servidores debe estar restringido al personal autorizado. El personal de la Institución deberá tener su carné de identificación siempre en un lugar visible.

d) Establecer un medio de control de entrada y salida de visitas a la Sala de Servidores. Si fuera posible, acondicionar un ambiente o área de visitas (formato de visitas a la Sala de Servidores: anexo 12).

e) El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.

f) Establecer políticas para la creación de los password y establecer periodicidad de cambios de los mismos.

g) La seguridad de los terminales de un sistema en red debería ser controlados por medios de anulación del disk drive, puertos USB, DVD y CD-RW

cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.

h) Los ambientes ubicación de equipos de comunicación sensibles, deben estar libre de materiales de naturaleza inflamable o que impidan el normal monitoreo de los mismos.

i) Está prohibido el uso de cámaras fotográficas en la Sala de Servidores, caso contrario debe pedirse permiso por escrito de la Alta Dirección.

j) Asignar a una sola persona la responsabilidad de la protección de los equipos en cada unidad operativa bajo supervisión de su jefatura.

Administración de la Cintoteca:

a) Debe ser administrada bajo la lógica de un almacén. Esto implica ingreso y salida de medios magnéticos (sean cintas, disquetes cassettes, cartuchos, Discos removibles, CDs, DVD, etc.), obviamente teniendo más cuidado con las salidas.

b) La cintoteca, que es el almacén de los medios magnéticos (sean cintas, disquetes cassettes, cartuchos, Discos removibles, CDs, DVD, etc.) y de la información que contienen, se debe controlar para que siempre haya determinado grado de temperatura y de la humedad.

c) Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.

d) El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

8.1.4 Protección contra amenazas externas y ambientales

La mayor parte de las amenazas externas y ambientales no son controlables por parte del IMARPE, (ver inciso 3.1.5), en su análisis se deben definir medidas de seguridad para evitar impactos en la organización, tales como la pérdida total o parcial del sistema de información del IMARPE. Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.

Cualquier amenaza de seguridad presentada por premisas vecinas, como un incendio en el edificio vecino, goteo de agua en el techo o en pisos ubicados por debajo del nivel de la tierra o una explosión en la calle.

Ejemplo

La sede central del IMARPE se ubica cerca al mar, estamos ante una amenaza de inundación.

Para evitar daño por inundación y por incendio es que se ha tomado las siguientes medidas:

a) La Sala de Servidores del IMARPE está provisto de alarmas contra incendio
b) La Sala de Servidores está protegido contra inundación ya que se encuentra totalmente en un ambiente cerrado.

8.2 Seguridad de los equipos

OBJETIVO: Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades del IMARPE. El equipo debería estar físicamente protegido de las amenazas y riesgos del entorno para reducir el riesgo de accesos no autorizados a los datos y protegerlo contra pérdidas o daños. También se debería considerar su instalación (incluyendo su uso fuera del local) y disponibilidad. Pueden requerirse medidas o controles especiales contra riesgos de accesos no autorizados y para proteger los sistemas de apoyo, como la alimentación interrumpida o la infraestructura de cableado.

8.2.1 Instalación y protección de equipos

Para la instalación y uso adecuado de los equipos de cómputo y comunicaciones se ha considerado los siguientes criterios:

- Ubicación en un lugar de bajo tráfico de personas o visitantes invitados a la institución para minimizar los riesgos de posibles amenazas.
- Acceso a la Sala de Servidores únicamente al personal autorizado, acondicionando una sala de visita si fuera el caso.
- Sistema de Aire acondicionamiento adecuado para la operación correcta de los servidores en el rango de la temperatura y humedad regulable.

- Ambiente libre de todo material inflamable para minimizar posible incendio, efectos negativos de agentes químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas, etc.
- No descuidar los elementos que requieren especial protección tales como:

Teclado. Mantener fuera del teclado grapas y clips, pues de insertarse entre las teclas, puede causar un cruce de función.

Cpu. Mantener la parte posterior del cpu liberado en por lo menos 10cm. Para asegurar así una ventilación mínima adecuada.

Mouse. Poner debajo del Mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste.

Protectores de pantalla. Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.

Caso HP LJ3005.

Caso HP Laserjet 4100 series tratar con cuidado y no apagar de súbito, asegurarse que el ON LINE esté apagado, así evitaremos problemas de cabezal y sujetador.

Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

8.2.1.1 Mantener las áreas Operativas limpias

Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas, para enunciarlas aquí. Sin embargo, algunos de los problemas que se puede evitar son: el peligro de fuego generado por la acumulación de papeles bajo el falso piso, el daño potencial al equipo por derramar el café, leche, u otros líquidos en los componentes del sistema, el peligro de fuego que se presentan por el excesivo almacenamiento de hojas continuas, el peligro por fumar y las falsas alarmas creadas por detectores de humo. Estos son solamente algunos de los problemas encontrados en las áreas operativas con reglas poco estrictas de limpieza.

8.2.1.2 Protección de equipos, software, procedimientos y documentación

Proveer protección frente al fuego y almacenamiento exterior de suministros, software, procedimientos y documentación. Hemos tenido en cuenta las siguientes medidas de seguridad. Se ha previsto de tres extintores que cumpla las características técnicas (no daña el equipo, no deja residuo y sea inofensivo). Estos equipos antifuego son ideales para los equipos eléctricos y electrónicos.

Ventajas: No causa daño al equipo, por ser un gas, no deja huella después de usarlo, porque se desvanece en el medio ambiente.

Desventajas: El extintor su función principal para contrarrestar el fuego es de eliminar él oxigeno, por lo tanto para usarlo es recomendable usar máscaras.

Estos equipos tienen indicaciones de cómo utilizar y además deben recibir una capacitación por parte de los especialistas en equipos contra incendio, porque el mal uso puede provocar asfixia. Se debe tener en cuenta que el equipo contra incendio es para cuando el fuego sé está iniciando y no para apagar un incendio de grandes proporciones.

Lugares recomendables de que deben existir estos equipos en la Sede Central del IMARPE

01 en el pasadizo del tercer piso, antes de ingresar a la sala de servidores y en lugar visible.

01 en la sala del centro de cómputo, debe estar ubicado a la entrada de la puerta, recomendable a la margen derecha y un lugar visible

01 cerca del archivador de disquetes, cintas DAT, CD-ROM, y otros dispositivos de backup

Los lugares recomendables donde deben existir estos equipos en el local de la Av. Argentina del IMARPE, deberán ser de acuerdo al ambiente a habilitarse e implementarse para el resguardo del backup.

8.2.2 Suministro Eléctrico

Los equipos modernos de cómputo están dotados de excelentes circuitos y filtros para distribuir la corriente eléctrica en su interior. Pero no obstante su propia protección, toda computadora debe protegerse de las variaciones de los voltajes externos.

Lo 'normal' es colocar entre la PC y la red de energía pública, elementos de barrera como reguladores de voltaje y supresores de picos de voltaje (surge protector).

La creación de una instalación con pozo a tierra no es en sí misma una seguridad 100% que impedirá cualquier daño en el interior de tu computadora, ya que los componentes electrónicos pueden originarlo independientemente, por degradación o agotamiento de las sustancias con que se fabrican las partes. El polo a tierra sin embargo, atenúa el daño de una sobrecarga o cortocircuito, orientando el exceso de corriente hacia el exterior del sistema, protegiendo al operador.

El circuito eléctrico de alimentación de una computadora necesita normalmente tres líneas de alimentación: la fase, el neutro y la tierra.

En ciertos casos es necesario instalar a continuación una fuente de energía ininterrumpida o UPS, esto es cuando trabajamos con datos muy valiosos o delicados en el PC. Después del regulador /acondicionador o UPS se conecta la computadora.

Por otra parte, debes tener en cuenta que si el uso de tu equipo es doméstico o casero, (nos referimos a que lo tienes en zona de poca variación de voltaje) puedes utilizar el tomacorriente común de una casa u oficina. Pero si estas en zona industrial o tu equipo forman parte de un grupo de computadoras (Sala de Servidores), el circuito de energía eléctrica debe ser independiente, es decir habrá que crear una red eléctrica exclusiva para las computadoras partiendo de la caja de breakers.

El pozo a tierra. Las computadoras actuales se protegen muy bien gracias a los excelentes componentes de su fuente y los reguladores de voltaje

modernos. Pero el circuito con polo a tierra se vuelve imprescindible cuando la instalación es de tipo comercial (como la de una empresa)

8.2.2.1 Suministro para las estaciones de trabajo

- El suministro eléctrico, fuente de toma para las PCs y equipos de comunicación tanto en la sede central como en el local de la Av. Argentina, es la estandarizada e independiente de la distribución e instalaciones para los servicios en general.
- El voltaje en la línea estandarizada es monitoreado periódicamente por la Unidad de Informática en coordinación con la Unidad de logística.

8.2.2.2 Suministro para los servidores en la oficina 307

Esta controlado además de la línea estandarizada, por un estabilizador redundante (UPS de 6 KW de potencia cada uno). El monitoreo del UPS en consumo de energía e insumo de baterías, esta bajo la responsabilidad de la Unidad de Informática (área soporte).

8.2.2.3 Suministro del grupo electrógeno

Si se produce interrupción de la corriente eléctrica que provee electro norte (apagón general, u otro motivo), se pone en operación al grupo electrógeno Caterpillar de 137.8 KW de potencia continua, para la continuidad del negocio en las unidades operativas más críticas.

8.2.3 Seguridad del Cableado

En el IMARPE existen tres tipos de cableados:

- La seguridad del cableado para las líneas de energía eléctrica clasificada en línea tradicional y normalizada como fuente de poder para los equipos de cómputo, se efectúa mediante mantenimiento preventivo constante y correctiva eventual.
- La seguridad del cableado para línea telefónica, corre a cargo de la propia telefónica.

- La seguridad del cableado para la red de datos con seis años de vigencia en la sede central y tres años en la Av. Argentina, se conduce mediante la certificación estipulada en el expediente técnico de cada cual.

8.2.4 Mantenimiento de Equipos

La disponibilidad e integridad de los equipos se realiza mediante los siguientes controles:

- Diagnostico del estado del equipo por intermedio del grupo soporte, determinando o recomendando la intervención del área de Mantenimiento (Unidad de Logística).
- Comprobado la necesidad del servicio, se procede el mantenimiento preventivo con los insumos disponibles.
- Si el defecto amerita repuestos, el mantenimiento correctivo se efectúa con los existentes en stock. En otro caso, se procede a la compra de los mismos para atender al usuario.
- Si el mantenimiento requiere de servicio especializado fuera de la institución, en el término de la garantía o sin ella, el trámite se realiza con la debida documentación.

A continuación se muestra el formato de mantenimiento de equipos (ver Cuadro N° 25)

Cod. Patrim	Estado	Uso	Fecha de Adquisición	Antigüedad	Ultimo Mantenimiento	Proximo Mantenimiento

Cuadro N° 25: Formato de mantenimiento de equipos

8.2.5 Seguridad de equipos fuera de los locales del IMARPE

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del IMARPE, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente

a la suministrada dentro del ámbito del IMARPE para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del IMARPE, cuando sea conveniente.

8.2.6 Seguridad en el rehúso o eliminación de equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

8.2.7 Retiro de la propiedad

Se deben considerar los siguientes controles:

1) El equipamiento, la información y el software no serán retirados de la sede del IMARPE sin autorización formal.
2) Los empleados(nombrados y contratados), y usuarios de terceros que tengan autoridad para permitir el retiro de la propiedad de los activos deben ser claramente identificados
3) Los tiempos limite para el retiro de equipos deben ser fijados y el retorno del equipo verificado para asegurar la conformidad}
4) El equipo debe ser registrado, si es necesario y apropiado, cuando este sea removido fuera del local así como cuando sea devuelto.

9. GESTIÓN DE COMUNICACIONES Y OPERACIONES

9.1 Procedimientos y responsabilidades de operación

OBJETIVO: Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Se implantará la segregación de tareas (ver inciso 9.1.4), cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

9.1.1 Documentación de procedimientos operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) Procesamiento y manejo de la información.
b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
d) Restricciones en el uso de utilitarios del sistema.
e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
f) Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
g) Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.
h) Creación y entrega de cuentas a cada usuario, se realiza a través de correo electrónico en la fase temporal, alcanzando su confidencialidad con el cambio de password a decisión del usuario.

i) Las interrupciones en el servicio de Internet por razones de mantenimiento u otras causas, son avisadas mediante comunicados autorizados por la Alta Dirección.

j) La cuota de espacio en el disco del servidor de correo, tiene un máximo con alerta automático en caso que el usuario se exceda a tal cuota.

k) Por disposición de la Alta Dirección está restringido o prohibido el uso de Messenger.

l) El antivirus corporativo se adquiere mediante un contrato con uso de licencia y se actualizan automáticamente o manualmente cuando ocurre cambio de versión.

Se mantiene actualizado el cuadro estadístico de los servidores. Ver anexo 1

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.

b) Instalación y mantenimiento de las plataformas de procesamiento.

c) Monitoreo del procesamiento y las comunicaciones.

d) Inicio y finalización de la ejecución de los sistemas.

e) Programación y ejecución de procesos.

f) Gestión de servicios.

g) Resguardo de información (Backup).

h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.

i) Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.

j) Uso del correo electrónico.

9.1.2 Gestión de cambios

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se retendrá un registro de auditoria que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.

b) Evaluación del posible impacto de dichos cambios.

c) Aprobación formal de los cambios propuestos.

d) Planificación del proceso de cambio.

e) Prueba del nuevo escenario.

f) Comunicación de detalles de cambios a todas las personas pertinentes.

g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos

9.1.3 Procedimientos de Manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad (Ver también 7.2.3. Comunicación de Incidentes Relativos a la Seguridad). Se deben considerar los siguientes ítems:

a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo

1. Fallas operativas
2. Código malicioso
3. Intrusiones
4. Fraude informático
5. Error humano
6. Catástrofes naturales

b) Contemplar y definir todos los tipos probables de incidentes relativos a Comunicar los incidentes a través de canales gerenciales apropiados tan pronto como sea posible, de acuerdo a lo indicado en 7.2.3 – "Comunicación de Incidentes Relativos a la Seguridad".

c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):

1. Definición de las primeras medidas a implementar
2. Análisis e identificación de la causa del incidente.
3. Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
4. Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
5. Notificación de la acción a la autoridad y/u Organismos pertinentes.

d) Registrar pistas de auditoria y evidencia similar para:

1. Análisis de problemas internos.
2. Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial (Ver 14.1. Cumplimiento de Requisitos Legales).
3. Negociación de compensaciones por parte de los proveedores de software y de servicios.

e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:

1. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
2. Documentación de todas las acciones de emergencia emprendidas en forma detallada.
3. Comunicación de las acciones de emergencia al comité de contingencia y seguridad y revisión de su cumplimiento.

4. Constatación de la integridad de los controles y sistemas del IMARPE en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Legal del IMARPE en el tratamiento de incidentes de seguridad ocurridos.

9.1.4 Segregación de tareas

Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se pudiera cumplir en algún caso, se implementarán controles como:

a) Monitoreo de las actividades
b) Registros de auditoria y control periódico de los mismos.
c) Supervisión por parte de la Unidad de Auditoria Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.

Asimismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.

Se asegurará la independencia de las funciones de auditoria de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

a) Separar actividades que requieren de connivencia para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.
b) Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

9.1.5 Separación de los recursos para desarrollo y producción

Los ambientes de desarrollo, prueba y producción, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de producción, en diferentes ambientes de operaciones, equipos, o directorios.

b) Separar las actividades de desarrollo y prueba, en entornos diferentes.

c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.

d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

e) Definir propietarios de la información para cada un de los ambientes de procesamiento existentes.

f) El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deberán implementarse los controles indicados en el punto “Separación de Tareas”.

En el Anexo 13 se presenta un esquema modelo de segregación de ambientes de procesamiento.

9.2 Gestión de servicios externos

OBJETIVO: Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos de terceros.

La organización debe verificar la implementación de acuerdos, el monitoreo de la conformidad con los acuerdos y los cambios gestionados con el fin de asegurar que todos los servicios entregados cumplen con todos los requerimientos acordados con terceros.

9.2.1 Servicio de entrega

El servicio entregado por terceros debe incluir los arreglos de seguridad acordados, definiciones de servicio y aspectos de la gestión del servicio. En este caso de arreglos de outsourcing, el IMARPE debe planear las transiciones (de información, recursos del procesamiento de información y cualquier otra cosa que requiere ser movido), y debe asegurar que la seguridad sea mantenida a través del periodo de transición.

El IMARPE debe asegurarse que los terceros mantengan una capacidad suficiente junto con planes realizables designados para asegurar que los niveles continuos del servicio acordado sean mantenidos siguiendo fallas mayores del servicio o desastre (véase 13.1).

9.2.2 Monitoreo y revisión de los servicios externos

El monitoreo y la revisión de los servicios externos debe asegurase que todos los términos de seguridad de la información y las condiciones de los acuerdos han sido adheridos, y que los incidentes y problemas en la seguridad de información han sido manejados propiamente. Esto debe implicar una relación y proceso de gestión del servicio entre el IMARPE y terceros para:

a) Servicio de monitoreo de niveles de funcionamiento para verificar que se adhieran a los acuerdos

b) Reportes de revisión de servicio producidos por terceros y que arregle reuniones regulares de progreso como requieran los acuerdos

c) Proveer información acerca de los incidentes de seguridad de información y revisión de esta información por terceros y el IMARPE como requiera los acuerdos y cualquier pauta de apoyo y procedimientos.

d) Revisar acuerdos y los rastros de intervención de los eventos de seguridad, problemas operacionales, fallas, trazabilidad de fallas e interrupciones relacionadas con el servicio entregado.

e) Resolver y manejar cualquier problema identificado.

9.2.3 Gestionar cambios para los servicios externos

El proceso de gestionar cambios para los servicios externos se necesita tomar en cuenta lo siguiente:

a) Cambios realizados por la organización para implementar :
   1) Realces en el actual servicio ofrecido
   2) Desarrollo de cualquier aplicación o sistema nuevo
   3) Modificaciones o actualizaciones de las políticas y procedimientos organizacionales
   4) Controles nuevos para resolver incidentes en la seguridad de información

b) Cambios en los servicios externos para implementar:
   1) Cambios y realces en el actual servicio ofrecido
   2) El uso de nuevas tecnologías
   3) Adopción de nuevos productos o versiones o lanzamientos nuevos
   4) Nuevas herramientas y ambientes de desarrollo
   5) Cambios de la locación física de los recursos de servicio
   6) Cambios en el vendedor

9.3 Planificación y aceptación del sistema

OBJETIVO: Minimizar el riesgo de fallos de los sistemas. Deberían realizarse proyecciones de los requisitos futuros de capacidad para reducir el riesgo de sobrecarga del sistema. Se debería establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los sistemas nuevos. Se deberían coordinar y revisar

regularmente los requisitos de recuperación de caídas de los servicios que soportan aplicaciones múltiples.

9.3.1 Planificación de la capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información del IMARPE para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva. Ver Anexo 3.

9.3.2 Aceptación del sistema

- Se realizan pruebas de procedimientos de los módulos en desarrollo del modulo IMARSIS (Pelágicos, Demersales).
- Se encuentra en proceso de mantenimiento el manual del usuario del IMARSIS
- Los cambios en las nuevas instalaciones afectan en sentido positivo.
- El proceso de desarrollo se realiza en estricta coordinación con los usuarios.
- Plan de continuidad del negocio como se requiere en el inciso 13.1
- Otros proyectos de sistemas de información: por cambio de tecnologías, licencia vencidas, etc.

9.4 Protección contra software malicioso

OBJETIVO: Proteger la integridad del software y de la información. Se requieren ciertas precauciones para prevenir y detectar la introducción de software malicioso. El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, “gusanos de la red”, “caballos de troya” y “bombas lógicas”. Los usuarios deberían conocer los peligros que puede ocasionar el

software malicioso o no autorizado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción. En particular es esencial que se tomen precauciones para detectar o evitar los virus informáticos en los computadores personales.

9.4.1 Medidas y controles contra software malicioso

El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementarán dichos controles.

El Responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por el IMARPE (Ver 14.1.2 Derecho de Propiedad Intelectual del Software).

b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.

c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.

d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del IMARPE, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.

f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

h) Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

9.5 Gestión interna de respaldo y recuperación

OBJETIVO: Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación. Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo (véase el apartado 12.1) haciendo copias de seguridad, ensayando su oportuna recuperación, registrando eventos o fallos y monitoreando el entorno de los equipos cuando proceda.

9.5.1 Recuperación de la información

El Responsable del Área de Soporte Técnico y el de Seguridad Informática junto al jefe de la Unidad de Informática y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información. Ver Anexo 15: Procedimiento y Política de Backup

El Responsable del Área Soporte dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Ver Anexo 16: Procedimiento y Política de Restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del IMARPE. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del IMARPE, según el punto “Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del IMARPE.” de esta política.

Se definirán procedimientos generales para el resguardo de la información, que deberán considerar los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.

c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en la sede Central. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el IMARPE. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad (Ver 6.2. Clasificación de la información) y requisitos legales a los que se encuentre sujeta.

d) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.

e) Probar periódicamente los medios de resguardo.

f) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Los procedimientos de realización de copias de resguardo y su almacenamiento deberán respetar las disposiciones del punto 6. Clasificación y Control de Activos y 14.1.3. Protección de los Registros del IMARPE de la presente Política.

Para mayor detalle ver Anexo 5: Servidores y estaciones de trabajo considerado en el proceso de backup (sede central y Av. Argentina).

9.5.2 Registro de Actividades del Personal Operativo

El Responsable del Área de Soporte Técnico de Unidad de Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Tiempos de inicio y cierre del sistema.

b) Errores del sistema y medidas correctivas tomadas.

c) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.

d) Ejecución de operaciones críticas

e) Cambios a información crítica

La Unidad de Auditoria Interna o quien sea propuesto por el Comité de Contingencia y Seguridad de la Información contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

9.5.3 Registro de Fallas

El Responsable del Área de Soporte Técnico de la Unidad de Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.

Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.

c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

9.6 Gestión de Seguridad de Redes

OBJETIVO: Asegurar la información en las redes y la protección de su infraestructura de apoyo. La gestión de la seguridad de las redes que cruzan las fronteras de la organización requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas.

9.6.1 Controles de red

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del IMARPE, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto "Asignación de Responsabilidades en Materia de Seguridad de la Información".

b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Área de Soporte Técnico de la Unidad de Informática implementará dichos controles.

9.7 Utilización y seguridad de los medios de información

OBJETIVO: Evitar daños a los activos e interrupciones de las actividades de la organización. Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema, de daño, robo y acceso no autorizado.

9.7.1 Gestión de medios removibles

El Responsable del Área de Soporte Técnico de la Unidad de Informática, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al capítulo 10 – "Control de Accesos".

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el IMARPE. (Ver inciso 8.2.6 Desafectación o Reutilización Segura de los Equipos.).

b) Requerir autorización para retirar cualquier medio del IMARPE y realizar un control de todos los retiros a fin de mantener un registro de auditoria.

c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Se documentarán todos los procedimientos y niveles de autorización, en concordancia con el capítulo 6. Clasificación y Control de Activos.

9.7.2 Eliminación de medios

El Responsable del Área de Soporte Técnico de la Unidad de Informática, junto con el Responsable de Seguridad Informática definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.

b) Voces u otras grabaciones.

c) Papel carbónico.

d) Informes de salida.

e) Cintas de impresora de un solo uso.

f) Cintas magnéticas.

g) Discos o casetes removibles.

h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).

i) Listados de programas.

j) Datos de prueba.

k) Documentación del sistema.

Asimismo, se debe considerar que podría ser más eficiente disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.

9.7.3 Procedimientos de manipulación de la información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a la clasificación establecida en el capítulo 6 – "Clasificación y Control de Activos".

En los procedimientos se contemplarán las siguientes acciones:

a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.

b) Restringir el acceso solo al personal debidamente autorizado

c) Mantener un registro formal de los receptores autorizados de datos

d) Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.

e) Proteger los datos en espera ("colas").

f) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

9.7.4 Seguridad de la documentación de sistemas

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:

a) Almacenar la documentación del sistema en forma segura.

b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

9.8 Intercambio de información y software

OBJETIVO: Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

Se deberían controlar los intercambios de información y software entre organizaciones, que deberían cumplir con toda la legislación correspondiente (véase el capítulo 14). Se deberían realizar los intercambios sobre la base de acuerdos formales. Se deberían establecer procedimientos y normas para proteger los medios en tránsito. Se considerarán las implicancias de seguridad asociadas al comercio, correo e intercambio electrónico de datos (EDI), así como los requisitos para las medidas y controles de seguridad.

9.8.1 Políticas y procedimientos para el intercambio de información y software

Los procedimientos y controles ha ser seguidos cuando se utilice instalaciones electrónicas de comunicación para el intercambio de información deben considerar lo siguiente:

a) Los procedimientos designados para proteger la información intercambiada de una intercepción, copiado, modificación, cambio de ruta y destrucción

b) Los procedimientos para la detección y protección contra código malicioso que pueden ser transmitido a través del uso de comunicación electrónica (véase el inciso 9.4.1)

c) Los procedimientos para proteger información electrónica sensible que esta en forma de archivo adjunto

d) Las políticas o pautas para el uso aceptable de las instalaciones de comunicación electrónica (véase el inciso 6.1.3)

e) Los procedimientos para el uso de comunicaciones inalámbricas, tomando en cuenta los riesgos particulares envueltos

f) Las responsabilidades de los empleados, contratistas y cualquier otro usuario de no comprometer al IMARPE, por difamación, hostigamiento, personificación, reenvió de cadenas de correos, compra no autorizada, etc.

g) Las pautas de disposición y retención para toda la correspondencia de negocios, incluyendo mensajes, en concordancia con la legislación y las regulaciones nacionales y locales.

h) No dejar información crítica o sensible en las instalaciones de impresión, como impresoras, copiadoras y faxes, ya que estas pueden ser accesadas por personal no autorizado.

i) Los controles y restricciones asociados con el reenvió de las instalaciones de comunicación como por ejemplo el reenvió automático de correos electrónicos a una dirección de correo externa

j) Recordar al personal que deben de tomar precauciones como por ejemplo no revelar información sensible con el fin de evitar ser escuchado o interpretado cuando hagan una llamada telefónica mediante:

1) Personas vecinas particularmente cuando se utiliza teléfonos móviles.
2) Intercepción de teléfonos y otras formas de oír comunicaciones a través de acceso físico al equipo o a la línea telefónica, o utilizando equipos de recepción de escaneo.
3) Personas al final del receptor

k) No dejar mensajes conteniendo información sensible en las maquinas contestadoras ya que estas pueden ser reproducidas por personas no autorizadas, guardadas en sistemas comunales o grabadas incorrectamente como resultado de un mal discado

l) Recordar al personal sobre los problemas de usar las maquinas de fax, nombrando:

1) El acceso no autorizado para crear almacenes de mensajes con el fin de recuperarlos.

2) La programación deliberada o accidentada de las maquinas para enviar mensajes a números específicos.

3) Envío de documentos y mensajes a un número equivocado por un mal discado o por el uso de un número mal grabado.

m) Recordar al personal no registrar datos demográficos, como la dirección de correo u otra información personal en cualquier software para evitar su uso no autorizado.

n) Recordar al personal que los fax modernos y las fotocopiadoras tienen páginas caché y paginas almacenadas en caso de que el papel se trabe y lo imprimirá una vez que se corrija el error.

9.8.2 Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información del IMARPE involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.

b) Procedimientos de notificación de emisión, transmisión, envío y recepción.

c) Normas técnicas para el empaquetado y la transmisión.

d) Pautas para la identificación del prestador del servicio de correo.

e) Responsabilidades y obligaciones en caso de pérdida de datos.

f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.

g) Términos y condiciones de la licencia bajo la cual se suministra el software.

h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.

i) Normas técnicas para la grabación y lectura de la información y del software.

j) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

9.8.3 Medios físicos en transito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar:

a) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.

b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes y/o proveedores.

c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:

1. Uso de recipientes cerrados.
2. Entrega en mano.
3. Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
4. En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

9.8.4 Seguridad del Gobierno Electrónico

El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto “Aprobación del Sistema” incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

a) Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del usuario y el IMARPE.

b) Autorización: Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica.

c) Procesos de oferta y contratación pública: Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.

d) Trámites en línea: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.

e) Verificación: Grado de verificación apropiado para constatar la información suministrada por los usuarios.

f) Cierre de la transacción: Forma de interacción más adecuada para evitar fraudes.

g) Protección a la duplicación: Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

h) No repudio: Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.

i) Responsabilidad: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

Las consideraciones mencionadas se implementarán mediante la aplicación de las técnicas criptográficas enumeradas en el punto "Política de Utilización de Controles Criptográficos." y tomando en cuenta el cumplimiento de los requisitos legales emanados de toda la normativa vigente.

Se darán a conocer a los usuarios, los términos y condiciones aplicables.

9.8.5 Seguridad del Correo Electrónico

Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.

b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.

c) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.

d) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la Terminal receptora o de la red a la que se encuentra conectada.

e) El impacto de un cambio en el medio de comunicación en los procesos del IMARPE.

f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.

g) Las implicancias de la publicación externa de listados de personal, accesibles al público.

h) El acceso de usuarios remotos a las cuentas de correo electrónico.

i) El uso inadecuado por parte del personal.

Política de Correo Electrónico

El Responsable de Seguridad Informática junto con el Responsable del Área de soporte técnico de la Unidad de Informática definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.

b) Protección de archivos adjuntos de correo electrónico.

c) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver 11.3. Controles Criptográficos).

d) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.

e) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

f) Aspectos operativos para garantizar el correcto funcionamiento del servicio (Ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).

g) Definición de los alcances del uso del correo electrónico por parte del personal del IMARPE.

h) Potestad del IMARPE para auditar los mensajes recibidos o emitidos por los servidores del IMARPE, lo cual se incluirá en el "Compromiso de Confidencialidad" (7.1.3. Compromiso de Confidencialidad)

Estos dos últimos puntos deben ser leídos a la luz de las normas vigentes que no sólo prohíben a los empleados a hacer uso indebido o con fines particulares del patrimonio estatal sino que también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento. (14.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información).

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el IMARPE debe informar claramente a sus empleados: a) cuál es el uso que el IMARPE espera que los empleados hagan del correo electrónico provisto por el IMARPE; y b) bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

9.8.6 Sistemas de Información de Negocios

Las consideraciones dadas a la seguridad e implicaciones de seguridad de interconectar dichas instalaciones, deben incluir:

a) Vulnerabilidades conocidas en los sistemas de administración: Logística, SIGA, SIAF, PDT601 y contabilidad donde la información es compartida por los diferentes partes del IMARPE

b) Vulnerabilidades de información en sistema de comunicación de negocios, como el grabado de llamadas telefónicas o de conferencia, las llamadas confidenciales, el almacenamiento de faxes, el correo abierto, la distribución de correo

c) Políticas y controles apropiados para manejar información compartida

d) Excluir categorías de información sensible y clasificar documentos si los sistemas no proveen un nivel apropiado de protección (véase el inciso 6.2)

e) Acceso restringido a la información diaria relacionado con individuos selectos, como el personal que trabaja en proyectos sensibles

f) Categorías de personal, contratistas o socios de negocios a los que se les permite el uso del sistema y de las locaciones desde donde puede ser accesado (véase 5.2)

g) Instalaciones restringidas seleccionadas para categorías de usuarios específicas

h) identificación del estado de usuarios, como empleados de la organización o contratistas en los directorios para beneficios de otros usuarios

i) Retención y soporte de la información colgada en el sistema (véase el inciso 9.5.1)

j) requisitos en el retraso y en los arreglos (véase capitulo 13)

9.9 Servicio de correo electrónico

OBJETIVO: Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

Las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo transacciones en línea y los requisitos para los controles. La integridad y disponibilidad de la información electrónica publicada a través del sistema disponible de publicidad deben ser también consideradas

9.9.1 Comercio electrónico

El propósito de esta política es presentar un esquema para el comportamiento aceptada cuando se realizan actividades de comercio electrónico (e-commerce).

Los controles definidos, tienen el propósito de proteger el comercio electrónico de numerosas amenazas de la red que puedan resultar en actividad fraudulenta y divulgación o modificación de la información:

a) Se aplica a todos los empleados del IMARPE involucrados con el comercio electrónico y a los socios de comercio electrónico del IMARPE. Los socios del comercio electrónico del IMARPE incluyen las direcciones, jefaturas y laboratorios de la organización, los clientes, socios comerciales y otros terceros.

b) El IMARPE debe asegurar la claridad de toda la información documentada y divulgar la información necesaria para asegurar el uso apropiado del comercio electrónico. El IMARPE y los socios del comercio electrónico deben someterse a la legislación nacional sobre el uso de la información de clientes y las estadísticas derivadas.

c) Los documentos y transacciones electrónicas usadas en el comercio electrónico debe ser legalmente admisibles. Las direcciones, jefaturas y laboratorios deben demostrar que sus sistemas de cómputo funcionan adecuadamente para establecer la autenticación de los documentos y transacciones legales. Los sistemas de información usados deben de estar de acuerdo con los estándares de seguridad corporativos antes de estar disponibles en producción.

d) Los sistemas de comercio electrónico deben publicar sus términos de negocios a los clientes. El uso de autoridades de certificación y archivos confiables de terceros deben estar documentados, de acuerdo con la política de seguridad de información del IMARPE.

e) Actividades de roles y responsabilidades entre el IMARPE y los socios de comercio electrónico deben de establecerse, documentarse y ser soportadas de los términos de transacciones

f) Asegurar que los socios de negocio se encuentran totalmente informados de sus autorizaciones

9.9.2 Transacciones en Línea

Las consideraciones de seguridad para las transacciones en línea incluir lo siguiente:

a) El uso de firmas electrónicas por cada una de las partes envueltas en la transacción

b) Todos los aspectos de la transacción, asegurando que:

   1) Las credenciales de usuario de todas las partes son validadas y verificadas

   2) La Transacción quede confidencial

   3) La privacidad asociada con todas las partes es retenidas

c) Los méritos de comunicación entre todas las partes implicadas deben ser cifrados.

d) Los protocolos utilizadas para comunicarse entre todas las partes debe ser seguro

e) Asegurar que el almacenamiento de los detalles de la transacción estén localizados fuera de cualquier ambiente público, como en una plataforma de almacenamiento existente en el Intranet de la organización, y que no sea retenidas ni expuesta en un medio de almacenamiento al que se puede acceder por Internet.

f) Cuando una autoridad confiable sea usada (para propósitos de publicar o mantener firmas digitales y/o certificados digitales) la seguridad es integrada a través de todo proceso de gestión de certificado/firma.

9.9.3 Sistemas Públicamente Disponibles

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación del IMARPE que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la

jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica.

Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Todos los sistemas de acceso público deberán prever que:

a) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales.

b) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.

c) La información sensible sea protegida durante el proceso de recolección y su almacenamiento.

d) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.

e) Se registre al responsable de la publicación de información en sistemas de acceso público.

f) La información se publique teniendo en cuenta las normas establecidas al respecto.

g) Se garantice la validez y vigencia de la información publicada.

9.10 Monitoreo

OBJETIVO: Detectar las actividades de procesamiento de información no autorizada.

Los sistemas deben ser monitoreados y los eventos de la seguridad de información deben ser grabadas. El registro de los operadores y el registro de la averías debe ser usado para asegurar que los problemas del sistema de información sean identificados.

El IMARPE debe cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades.

El monitoreo del sistema debe ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad de un acceso a un modelo de política.

9.10.1 Registro de la auditoria

Los registros de auditoria deben incluir, lo siguiente:

a) Identificaciones de usuarios

b) Fecha y hora de conexión y desconexión

c) Identidad del Terminal o locación si es posible

d) Registro de éxito o fracaso de los intentos de acceso al sistema

e) Registro de éxito o fracaso de datos y de otros intentos de accesos a recursos

f) Cambios de la configuración del sistema

g) Uso de privilegios

h) Uso de las instalaciones y aplicaciones del sistema

i) Archivos accesados y el tipo de acceso

j) direcciones de red y protocolos

k) Las alarmas realizadas por el sistema de control de accesos

l) Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusos

9.10.2 Monitoreando el uso del sistema

El monitoreo de control de los sistemas se deben incluir.

a) Acceso autorizado, incluyendo detalles como:
   1) La identificación del usuario
   2) La fecha y hora de los eventos claves
   3) El tipo de eventos
   4) Los archivos ingresados
   5) El programa y recurso utilizado

b) Todas las operaciones privilegiadas, como:
   1) Uso de cuentas privilegiadas, como supervisores, administradores

2) Puesta en marcha y parada del sistema

3) Conexión o desconexión de un recurso de entrada o salida

c) Intentos de acceso no autorizados, como:

1) Intentos fallidos

2) Acciones con fallas o rechazadas que involucran datos y otros recursos

3) Violaciones a las políticas de acceso y las notificaciones de los firewalls y entrada de red

4) Las alertas de los sistemas de dirección de intrusos del propietario;

d) Alertas o Fallas del sistema como:

1) Alertas o mensajes de consolas

2) Excepciones de registro en el sistema

3) Alarmas de la gerencia de red

4) Alarmas levantadas por los sistemas de control de accesos.

e) Cambios o intentos de cambio a la configuración y controles de los sistemas de seguridad

El numero de veces que deberán ser revisados las actividades de monitoreo debe depender de los riesgos implicados. Los factores de riesgo que deben ser considerados incluyen:

a) Criticidad de los procesos de aplicación

b) Valor, sensibilidad y criticidad de la información implicada

c) Experiencia pasadas de infiltraciones del sistema y mal uso y la frecuencia de las vulnerabilidades explotadas

d) Extensión de la interconexión del sistema(particularmente redes publicas)

e) Registro de la instalación que esta siendo desactivada

9.10.3 Protección de la información de registro

Los controles deben proteger contra cambios no autorizados y problemas operacionales con la instalación de registro incluyendo:

a) Alteraciones a los tipos de mensaje que son grabados

b) Archivos de registro editados o eliminados

c) La capacidad de almacenamiento del medio del archivo de registro que ha sido excedido, resultando en la falla de los eventos almacenados o la sobre escritura de eventos pasados

9.10.4 Registro de administradores y operadores

Los registros deben incluir:

a) El tiempo en que ocurrió el evento

b) Información acerca del evento o fallas

c) Contabiliza que administrador u operador fue implicado

d) Que procesos fueron implicados

Los registros de los administradores y usuarios del sistema deben ser revisados en una base regular (recomendable mensualmente)

9.10.5 Registro de Avería

Las averías reportadas por usuarios o por programas del sistema relacionados con problemas en el procesamiento o comunicación de información, deben ser registradas. Deben existir reglas para maniobrar las averías reportadas incluyendo:

a) Revisión de los registros de averías para asegurar que las fallas han sido resuelta satisfactoriamente

b) Revisión de las medias correctivas para asegurar que los controles no han sido comprometido y que la acción realizada es totalmente autorizada

Se debe asegurar que el registro de error es activado, si es que se encuentra disponible en el sistema.

10. CONTROL DE ACCESOS

10.1 Requisitos de negocio para el control de accesos

OBJETIVO: Controlar los accesos a la información. Se debería controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad. Se deberían tener en cuenta para ello las políticas de distribución de la información y de autorizaciones. Ver apartado 10.3.

10.1.1 Política de control de accesos

- Proporcionar información fuera y dentro de la institución previa autorización de la Alta Dirección.
- Respetar el derecho de autor en todo nivel, en copia de documentos, datos, Software, etc.
- No dejar abierto una sesión en la computadora a la que se tiene acceso. Activar un password que limite el acceso de terceros.
- Las cuentas de correo proveídos por la institución, solo deben ser utilizados en actividades netamente laborales.
- Evitar el reenvió de correos de contenido publicitario, político, comercial u otro que no esta referido al que hacer de la institución.
- Establecer y respetar el calendario de modificación de password de la administración de los servidores.
- Instalar Software autorizado por la institución incluida los que se descarga por Internet.
- Mantener actualizado el inventario de Software en coordinación con la Unidad de Logística.
- Mantener privacidad acerca de los contenidos de los datos e información administrados por los sistemas institucionales.
- Mantener vigente la identificación impuesta por la Unidad de Logística en los activos de la institución.

10.2 Gestión de acceso de usuarios

OBJETIVO: Asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información.

Establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de la red de Informática del IMARPE

Estos procedimientos deben cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de nuevos hasta la baja del registro de usuarios que ya no requieran dicho acceso a los sistemas y servicios de la Red de Informática del IMARPE. Se debe prestar especial atención, donde sea apropiado, al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios.

10.2.1 Registro de usuarios

El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.

b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.

c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del IMARPE, por ejemplo que no compromete la separación de tareas.

d) Entregar a los usuarios por escrito sus derechos de acceso.

e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

g) Mantener un registro formal de todas las personas autorizadas para utilizar el servicio.

h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del IMARPE o sufrieron la pérdida/robo de sus credenciales de acceso.

i) Efectuar revisiones periódicas con el objeto de:

- Cancelar identificadores y cuentas de usuario redundantes
- Inhabilitar cuentas inactivas por un periodo mayor a 60 días
- Eliminar cuentas inactivas por un periodo mayor a 120 días

En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

k) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

10.2.2 Gestión de privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos software.

b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.

c) Mantener un proceso de autorización y un registro de todos los privilegios asignados.

d) Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

e) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados (recomendable cada 30 días).

f) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática.

10.2.3 Gestión de contraseñas de usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad (Ver 7.1.3. Compromiso de Confidencialidad)

b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.

c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.

d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.

e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad Informática conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determine necesario (o lo justifique).

f) Configurar los sistemas de tal manera que:

- Las contraseñas deben tener, recomendablemente, mínimo 8 caracteres
- Suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta, la rehabilitación deberá ser solicitada al administrador de las cuentas.
- Solicitar el cambio de la contraseña en el lapso no mayor a 90 días.
- Impedir que las últimas 12 contraseñas sean reutilizadas

10.2.4 Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como la instalación de plataformas o sistemas, habilitación de servicios, actualización de software,

configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

a) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
b) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
c) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
d) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
e) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad.

10.2.5 Revisión de los derechos de acceso a los usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares (mayor a 6 meses), a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios a intervalos regulares (mayor a 6 meses).

b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos regulares (recomendable no mayor a 3 meses).

c) Revisar las asignaciones de privilegios a intervalos regulares (recomendable no mayor a 6 meses), a fin de garantizar que no se obtengan privilegios no autorizados.

10.3 Responsabilidades de los usuarios

OBJETIVO: Evitar el acceso de usuarios no autorizados a la información y a las instalaciones del procesamiento de información.

Una protección eficaz necesita la cooperación de los usuarios autorizados. Los usuarios deberían ser consientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

Un escritorio limpio, así como una política de pantalla clara debe ser implementado con el fin de reducir el riesgo de acceso no autorizado o de daño a los papeles, medios e instalaciones del procesamiento de información.

10.3.1 Uso de contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de riesgo del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:

1. Sean fáciles de recordar.

2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").

f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

g) Notificar de acuerdo a lo establecido en 7.2.3 – "Comunicación de Incidentes Relativos a la Seguridad", cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

10.3.2 Equipo informático de usuario desatendido

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para

la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.

b) Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

10.3.3 Política de pantalla y escritorio limpio

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

b) Guardar bajo llave la información sensible o crítica del IMARPE (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.

c) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o

copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

d) Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.

e) Bloquear las fotocopiadoras (protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

10.4 Control de acceso a la red

OBJETIVO: Protección de los servicios de la red. Debería controlarse el acceso a los servicios a las redes internas y externas. Hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

a) Interfaces adecuadas entre la red de la organización y las publicas o las privadas de otras organizaciones

b) Mecanismos adecuados de autenticación para los usuarios y los equipos

c) Control de los accesos de los usuarios a los servicios de información

10.4.1 Política de uso de los servicios de la red

Las conexiones no seguras a los servicios de red pueden afectar a todo el IMARPE, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable del Área de soporte Técnico de la Unidad de Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa

(Direcciones, jefaturas, laboratorios) que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad del IMARPE.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.

b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política es coherente con la Política de Control de Accesos del IMARPE (Ver 10.1.1. Política de Control de Accesos).

10.4.2 Autenticación de usuario para conexiones externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información del IMARPE. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:

- Asignación de la herramienta de autenticación
- Registro de los poseedores de autenticadotes
- Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
- Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.

b) Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:

- Establecimiento de las reglas con el usuario.
- Establecimiento de un ciclo de vida de las reglas para su renovación.

c) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de re-llamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información del IMARPE. Al aplicar este tipo de control, el IMARPE no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no será posible aplicar el control de re-llamada. Asimismo, es importante que el proceso de re-llamada garantice que se produzca a su término, una desconexión real del lado del IMARPE.

10.4.3 Identificación de equipos en la redes

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación del IMARPE. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad del IMARPE. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio

alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

10.4.4 Diagnostico remoto y configuración de protección de puertos

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto “Autenticación de Usuarios para Conexiones Externas”.

10.4.5 Segregación de redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios (Ver 10.4.7. Control de Conexión a la Red y 10.4.8. Control de Ruteo de Red) y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos (Ver 10.1. Requisitos de negocio para el control de acceso).

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso (Ver 10.1. Requisitos de negocio para el control de acceso), el Responsable del Área Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados (Ver 10.4.7. Control de Conexión a la Red y 10.4.8. Control de Ruteo de Red) para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad Informática, el esquema más apropiado a implementar.

10.4.6 Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa(direcciones, jefaturas, laboratorios) a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares.

Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto “Compromiso de Confidencialidad”. Para ello, el Responsable de Seguridad Informática junto con el Responsable del Área de Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como son la instalación de “firewalls”, “proxies”, etc.

10.4.7 Control de Conexión a la Red

Sobre la base de lo definido en el punto "Requerimientos”, se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los “gateways” que separen los diferentes dominios de la red.

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a) Correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a la red fuera del horario laboral.

10.4.8 Control de Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del IMARPE, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos (Ver 10.1.1. Política de Control de Accesos). Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

10.4.9 Seguridad de los servicios de Red

El Responsable de Seguridad Informática junto con el Responsable del Área de soporte de la Unidad Informática definirán las pautas para garantizar la seguridad de los servicios de red del IMARPE, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Responsable de Seguridad Informática.

10.5 Control de acceso al sistema operativo

OBJETIVO: Evitar acceso no autorizados a los computadores.

Las prestaciones de seguridad a nivel de sistema operativo se deberían utilizar para restringir el acceso a los recursos del computador. Estos servicios deberían ser capaces de:

a) Identificar y verificar la identidad de cada usuario autorizado en concordancia con una política definida de control de acceso.
b) Registrar los accesos satisfactorios y fallidos al sistema
c) Registrar el uso de privilegios especiales del sistema
d) Alarmas para cuando la política del sistema de seguridad sea abierta
e) Suministrar mecanismos, adecuados de autenticación
f) Cuando proceda, restringir los tiempos de conexión de usuarios

10.5.1 Procedimientos de conexión de terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación deberá:

a) Mantener en secreto los identificadores de sistemas o aplicaciones en tanto se hayan llevado a cabo exitosamente el proceso de conexión.

b) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.

c) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.

d) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.

e) Limitar el número de intentos de conexión no exitosos permitidos y:

- Registrar los intentos no exitosos.
- Impedir otros intentos de identificación, una vez superado el límite permitido.
- Desconectar conexiones de comunicaciones de datos.

f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.

g) Desplegar la siguiente información, al completarse una conexión exitosa:

- Fecha y hora de la conexión exitosa anterior.
- Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

10.5.2 Identificación y autenticación del usuario

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para el IMARPE, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), deberá implementarse un procedimiento que incluya:

a) Asignar la herramienta de autenticación.

b) Registrar los poseedores de autenticadores.

c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.

d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

10.5.3 Sistema de gestión de contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas

de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.

b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.

c) Imponer una selección de contraseñas de calidad según lo señalado en el punto “Uso de Contraseñas”.

d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto “Uso de Contraseñas”.

e) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.

f) Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

g) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.

h) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.

j) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).

k) Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

10.5.4 Utilización de las facilidades del sistema

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a) Utilizar procedimientos de autenticación para utilitarios del sistema.
b) Separar entre utilitarios del sistema y software de aplicaciones.
c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
d) Evitar que personas ajenas al IMARPE tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
e) Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
f) Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.
g) Registrar todo uso de utilitarios del sistema.
h) Definir y documentar los niveles de autorización para utilitarios del sistema.
i) Remover todo el software basado en utilitarios y software de sistema innecesarios.

10.5.5 Desconexión automática de sesiones

El Responsable de Seguridad Informática, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad del IMARPE, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la Terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por

tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la Terminal.

Para las PC's, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

10.6 Control de acceso a las aplicaciones y la información

OBJETIVO: Prevenir el acceso no autorizado a la información contenida en los sistemas.

Se deberían usar las facilidades de seguridad lógica dentro de los sistemas de aplicación para restringir el acceso.

Se deberían restringir el acceso lógico al software y a la información solo a los usuarios autorizados. Las aplicaciones deberían:

a) Controlar el acceso de los usuarios a la información y las funciones del sistema de aplicación, de acuerdo con la política de control de accesos.
b) Protegerse de accesos no autorizados desde otras facilidades o software de sistemas operativos que sean capaces de eludir los controles del sistema o de las aplicaciones
c) No comprometer la seguridad de otros sistemas con los que se compartan recursos de información.

Para mayor detalle ver Anexo 7: Relación de usuarios vs. Acceso a las aplicaciones

10.6.1 Restricción de acceso a la información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política del

IMARPE para el acceso a la información, (Ver 10.1. Requisitos de negocio para el control de accesos).

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.

b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.

c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.

d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.

e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

10.6.2 Aislamiento de sistemas sensible

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad

puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

a) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación (Ver 6. Clasificación y Control de Activos).

b) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.

c) Coordinar con el Responsable del Área informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.

d) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.

e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

10.7 Informática móvil y trabajo remoto

OBJETIVO: Garantizar la seguridad de la información cuando se usan dispositivos de información móvil y teletrabajo.

La protección requerida debería ser proporcional a los riesgos que causan estas formas específicas de trabajo. Se deberá considerar los riesgos de trabajar en un entorno desprotegido cuando se usa informática móvil y aplicar la protección adecuada. En el caso del teletrabajo la organización deberá implantar protección en el lugar del teletrabajo y asegurar que existen los acuerdos adecuados para este tipo de trabajo.

10.7.1 Informática móvil y comunicaciones

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información del IMARPE. Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Disquetes, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc..

Esta lista no es taxativa, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial del IMARPE y por lo tanto, ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria

b) El acceso seguro a los dispositivos

c) La utilización de los dispositivos en lugares públicos.

d) El acceso a los sistemas de información y servicios del IMARPE a través de dichos dispositivos.

e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.

f) Los mecanismos de resguardo de la información contenida en los dispositivos.

g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

a) Permanecer siempre cerca del dispositivo.

b) No dejar desatendidos los equipos.

c) No llamar la atención acerca de portar un equipo valioso.

d) No poner identificaciones del Organismo en el dispositivo, salvo los estrictamente necesarios.

e) No poner datos de contacto técnico en el dispositivo.

f) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del IMARPE, los que incluirán:

a) Revocación de las credenciales afectadas

b) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

10.7.2 Trabajo remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al IMARPE.

El trabajo remoto sólo será autorizado por el Responsable de la Unidad Organizativa, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad Informática, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios del IMARPE, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio u oficina y del ambiente local.

b) El ambiente de trabajo remoto propuesto.

c) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del IMARPE, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.

d) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.

e) Evitar la instalación / desinstalación de software no autorizada por el IMARPE.

Los controles y disposiciones comprenden:

a) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.

b) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del IMARPE y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.

c) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.

d) Incluir seguridad física.

e) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.

f) Proveer el hardware y el soporte y mantenimiento del software.

g) Definir los procedimientos de backup y de continuidad de las operaciones.

h) Efectuar auditoria y monitoreo de la seguridad.

i) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

j) Asegurar el reingreso del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoria específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

11. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

11.1 Requisitos de seguridad de los sistemas

OBJETIVO: Asegurar que la seguridad esté imbuida dentro de los sistemas de información. Esto incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios. El diseño y la implantación de los procesos de negocio que soportan las aplicaciones o el servicio, pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados antes de desarrollar los sistemas de información. Todos los requisitos de seguridad, incluyendo las disposiciones para contingencias, deberían ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

11.1.1 Análisis y especificación de los requisitos de seguridad

Actualmente existen mecanismos que permiten el desarrollo y mantenimiento de sistemas, sin embargo los mismos deben ser evaluados para determinar su pertinencia. Si ese fuese el caso, se debería dar la aprobación correspondiente. Esta parte esta asociada al desarrollo de sistemas integrales para la seguridad institucional y por lo tanto al cumplimiento de las observaciones o recomendaciones de auditoria.

Se deben tener en cuenta las siguientes consideraciones:

a) Cada requerimiento de software o de un nuevo sistema debe ser comunicado a la Unidad de Informática. Esta es la responsable de

elevar un informe a la alta dirección de la Institución para evaluar su pertinencia. La pertinencia estará referida al control del desarrollo o del mantenimiento para que se cumplan las condiciones del contrato. Garantizar la entrega, registro y almacenamiento adecuado de la documentación producto y/o entregables del desarrollo o mantenimiento de los sistemas institucionales.

b) Se deberá emplear como documento base la metodología de desarrollo, así como los estándares de desarrollo definidos por la Unidad de Informática, los cuales deben ser aprobados por la alta dirección.

c) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoria, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.

d) La Unidad de Informática, con el respaldo de la alta dirección es la responsable de monitorear el cumplimiento de los contratos, registrar y recabar los entregables, monitorear el avance para el cumplimiento de los planes de acción y verificar la aplicación correcta de los documentos que sostengan el desarrollo o mantenimiento del sistema en cuestión.

e) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

11.2 Seguridad de las aplicaciones del sistema

OBJETIVO: Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones. Se deberían diseñar dentro de las aplicaciones (incluidas las aplicaciones escritas por los usuarios) las medidas de control y las evidencias de auditoria o los registros de actividad. Éstos deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida. Se pueden requerir medidas y controles adicionales en los sistemas que procesen o tengan impacto sobre activos sensibles, valiosos o críticos para la organización. Dichas medidas se deberían determinar a partir de los requisitos de seguridad y la evaluación de riesgos.

11.2.1 Validación de los datos de entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

a) Control de secuencia.

b) Control de monto límite por operación y tipo de usuario.

c) Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.

d) Control de paridad.

e) Control contra valores cargados en las tablas de datos.

f) Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

a) Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo

realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.

b) Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.

c) Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

11.2.2 Control del proceso interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

a) Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.

b) Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.

c) Procedimientos que establezcan la revisión periódica de los registros de auditoria y forma de detectar cualquier anomalía en la ejecución de las transacciones.

d) Procedimientos que realicen la validación de los datos generados por el sistema.

e) Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.

f) Procedimientos que controlen la integridad de registros y archivos.

g) Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.

h) Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención

de las actividades de procesamiento hasta que el problema sea resuelto.

11.2.3 Integridad de mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto “Controles Criptográficos”.

11.2.4 Validación de los datos de salida

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

a) Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.

b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.

c) Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.

d) Procedimientos para responder a las pruebas de validación de salidas.

e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

11.3 Controles Criptográficos

OBJETIVO: Proteger la confidencialidad, autenticidad o integridad de la información.

Se deberán usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

11.3.1 Política de uso de los controles criptográfico

El IMARPE establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

a) Se utilizarán controles criptográficos en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera del ámbito del IMARPE.
3. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.

b) Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

c) El Responsable del Área Informática propondrá la siguiente asignación de funciones(Cuadro N° 26)

Función	Cargo
Implementación de la Política de Controles Criptográficos	UI-Soporte técnico
Administración de Claves	UI-Soporte técnico

Cuadro N° 26: Formato de funciones

d) Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

1. Cifrado Simétrico

Algoritmo	Longitud de clave
AES(Advanced Encryption Standard)	128/192/256
3DES(Data Encryption Standard)	168 bits
IDEA(International Data Encryption Algorithm)	128 bits
RC4 (El RC4 es un algoritmo de cifrado de flujo diseñado por Ron Rivest para RSA Data Security)	128 bits
RC2(El RC2 es un algoritmo de cifrado por bloques de clave de tamaño variable diseñado por Ron Rivest de RSA Data Security (la RC quiere decir Ron's Code o Rivest's Cipher).	128 bits

Cuadro N° 27: Cifrado Simétrico

2. Cifrado Asimétrico

Caso de utilización	Algoritmo	Longitud de clave
Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 bits
Para certificados de sitio seguro	RSA	1024 bits
Para certificados de Certificador o de información de estado de certificados	RSA	2048 bits
Para certificados de usuario (personas físicas o Jurídicas)	RSA	1024 bits
Para digesto seguro	ECDSA SHA-1	160 bits 256 bits

Cuadro N° 28: Cifrado Asimétrico

Los algoritmos y longitudes de clave mencionados son los que a la fecha se consideran seguros. Se recomienda verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

11.3.2 Gestión de claves

Protección de Claves Criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte del IMARPE de los dos tipos de técnicas criptográficas, a saber:

a) Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

b) Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se aplicarán con éste propósito los algoritmos criptográficos enumerados en el punto 11.3.1. Política de Utilización de Controles Criptográficos.

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

Normas, Procedimientos y Métodos

Se redactarán las normas y procedimientos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.

b) Generar y obtener certificados de clave pública de manera segura.

c) Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.

d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.

e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.

f) Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula del IMARPE (en cuyo caso las claves también deben archivarse).

g) Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades del IMARPE, por ejemplo para la recuperación de la información cifrada.

h) Archivar claves, por ejemplo, para la información archivada o resguardada.

i) Destruir claves.

j) Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de (recomendable lapso no mayor a 12 meses).

Además de la administración segura de las claves secretas y privadas, deberá tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.

En consecuencia es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso es llevado a cabo por una entidad denominada Autoridad de Certificación (AC) o Certificador.

11.4 Seguridad de los archivos del sistema

OBJETIVO: Asegurar que los proyectos de Tecnología de la Información (TI) y las actividades complementarias sean llevadas a cabo de una forma segura. El acceso a los archivos del sistema debería ser controlado. El mantenimiento de la integridad del sistema debería ser responsabilidad del grupo de desarrollo o de la función del usuario a quien pertenezcan las aplicaciones del sistema o el software.

11.4.1 Control de software en producción

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada por el IMARPE o por un tercero tendrá un único Responsable designado formalmente por el Responsable de la Unidad de Informática.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

- El Responsable de la Unidad Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:

  a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

  b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

  c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.

  d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a) Guardar sólo los ejecutables en el ambiente de producción.

b) Llevar un registro de auditoria de las actualizaciones realizadas.

c) Retener las versiones previas del sistema, como medida de contingencia.

d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y la conformidad pertinentes, las pruebas previas a realizarse, etc.

e) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

f) Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

g)

11.4.2 Protección de los datos de pruebas del sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo (producción). Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

a) Prohibir el uso de bases de datos operativas (producción). En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.

b) Solicitar autorización formal para realizar una copia de la base operativa (producción) como base de prueba, llevando registro de tal autorización.

c) Eliminar inmediatamente, una vez completadas las pruebas, la información operativa (producción) utilizada.

11.4.3 Control de cambios de datos producción

La modificación, actualización o eliminación de los datos operativos (producción) serán realizados a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos (Ver 10.2. Gestión de Accesos de Usuarios). Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Responsable de Seguridad Informática definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

a) Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.

b) El Propietario de la Información afectada y el Responsable de Seguridad Informática aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.

c) Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas (Ver 10.2.4. Gestión de Contraseñas Críticas) y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.

d) Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales de acuerdo a lo establecido en 9.1.4. Separación de Funciones.

e) Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad Informática.

11.4.4 Control de acceso a los códigos de programas fuentes.

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

a) El Responsable de la Unidad de Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y deberá:

- Proveer al Área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
- Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
- Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
- Administrar las distintas versiones de una aplicación.
- Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

b) Denegar al "administrador de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia.

c) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.

d) Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.

e) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.

f) Evitar que la función de "administrador de programas fuentes" sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.

g) Prohibir el guardado de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.

h) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.

i) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el IMARPE en los procedimientos que surgen de la presente política.

11.5 Seguridad en los procesos de desarrollo y soporte

OBJETIVO: Mantener la seguridad del software de aplicación y la información. Se deberían controlar estrictamente los entornos del proyecto y de soporte. Los directivos responsables de los sistemas de aplicaciones también lo deberían ser de la seguridad del entorno del proyecto o su soporte. Se deberían asegurar de la revisión de todo cambio propuesto al sistema para comprobar que no debilite su seguridad o la del sistema operativo (producción).

11.5.1 Procedimientos de control de cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

a) Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.

b) Mantener un registro de los niveles de autorización acordados.

c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.

d) Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).

e) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.

f) Obtener aprobación formal por parte del Responsable de la Unidad de Informática para las tareas detalladas, antes que comiencen las tareas.

g) Solicitar la revisión del Responsable de Seguridad Informática para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.

h) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.

i) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.

j) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

k) Mantener un control de versiones para todas las actualizaciones de software.

l) Determinación de lugar, fecha, hora, recursos físicos y humanos requeridos para la implementación del cambio en el ambiente de producción.

m) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

n) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

o) Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo (producción), de acuerdo a lo establecido en "Control del Software Operativo". Ver anexo 14: modelo de control de cambios de sistemas de información y/o aplicativos

En el Anexo 13 del presente trabajo se presenta un esquema modelo de segregación de ambientes de procesamiento.

11.5.2 Revisión técnica de los cambios en el sistema operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.

c) Asegurar la actualización del Plan de Continuidad de las Actividades del IMARPE.

d) Mantener el sistema operativo actualizado, con los últimos parches de seguridad disponibles. Las actualizaciones críticas deben ser probadas antes de ser implementadas en el ambiente de producción, de manera de asegurarse de que los cambios no afecten la operatoria del sitio Web.

e) Configurar el sistema operativo de manera segura, implementando las mejores prácticas para el *hardening* de plataformas. Esto incluye, entre

otras actividades: deshabilitar cuentas de ejemplo, cambiar claves por defecto, etc.

Se le debe dar la responsabilidad, al personal del área de soporte técnico de la Unidad de Informática, de monitorear las vulnerabilidades y los lanzamientos de los parches y arreglos por parte de los vendedores (véase inciso 11.6)

11.5.3 Restricciones en los cambios a los paquetes de software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable de la Unidad de Informática, deberá:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Determinar la conveniencia de que la modificación sea efectuada por el IMARPE, por el proveedor o por un tercero.

c) Evaluar el impacto que se produce si el IMARPE se hace cargo del mantenimiento.

d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

11.5.4 Fuga de información

Se debe considerar lo siguiente para limitar el riesgo de fuga de información, como por ejemplo a través del uso y explotación de canales cubiertos:

a) Escaneo de medios de salida y comunicaciones para información oculta.

b) Implementar demodulación y enmascarado, y el comportamiento de las comunicaciones para reducir la probabilidad de que un tercero sea capaz de deducir información desde dicho comportamiento.

c) Haciendo uso de los sistemas y software que se consideran de alta integridad, por ejemplo productos evaluados(véase ISO/IEC 15408)

d) Monitoreo regular de las actividades del personal y del sistema, donde sea permitido bajo la legislación o regulación existente.

e) Monitoreo del uso de recursos en sistemas de computo.

f) Bloqueo físico de puertos de las computadoras: personales, portátiles, celulares; fortalecimiento de supervisión también como drásticas acciones tales como total prohibición de iPods y dispositivos similares en el sitio de trabajo. Sin embargo, ese no es el mejor acercamiento práctico al problema. Dispositivos portátiles de almacenamiento pueden ser herramientas beneficiosas para la fuerza laboral de la empresa y una prohibición podría ser contra productivo.

g) La opción ideal para asegurar el control completo sobre los dispositivos portátiles de almacenamiento es el implementar barreras tecnológicas tales como GFI EndPointSecurity. GFI EndPointSecurity es una solución que permite el control total sobre las transferencias de datos desde y hacia dispositivos portátiles de almacenamiento en toda la red y basado en usuario.

11.5.5 Desarrollo externo del software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos (Ver 14.1.2. Derechos de Propiedad Intelectual).

b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorias, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

d) Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto 5.2.3. Requisitos de seguridad en contratos en outsourcing.

e) Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

f) Se debe poner particular atención en la flexibilidad del software, su capacidad y magnitud de sus características de auditoria y confiabilidad.

g) El soporte y mantenimiento después de su desarrollo.

h) Se recomienda asesoría legal al contratar el desarrollo del software.

i) El contrato debe fijar claramente la propiedad del software para evitar disputa posterior.

j) Los términos del contrato deben proteger al IMARPE especificando cuando y como se terminará la prueba y cuando ocurrirá la implantación total.

11.6 Gestión de la vulnerabilidad técnica

OBJETIVO: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica debe ser implementada de una manera efectiva, sistemática y respetable con medidas tomadas para confirmar su efectividad. Estas consideraciones deben incluir los sistemas operativos y otras aplicaciones en uso.

11.6.1 Control de las vulnerabilidades técnicas

Una acción apropiada y a tiempo debe ser tomada en cuenta en respuesta a la identificación de vulnerabilidades técnicas potenciales. Las siguientes pautas deben seguirse para establecer un proceso de gestión de vulnerabilidades técnicas efectivas.

a) La Unidad de Informática encargará a un personal de área los roles y responsabilidad asociados con las gestión de vulnerabilidades técnicas, incluyendo el monitoreo de vulnerabilidades, la evaluación de la vulnerabilidad de riesgo, el parchado, el seguimiento de activos y cualquier otra responsabilidades coordinadas.

b) Los recursos de información que se utilizaran para identificar las vulnerabilidades técnicas relevantes y para mantener precaución sobre

ellos se deben identificar para el software y otras tecnologías (basadas en el inventario de activos, véase 6.1.1); estos recursos de información deben ser actualizados en cambios de inventario o cuando un recurso nuevo o mas útil se encuentre.

c) Se debe definir una línea de tiempo para reaccionar ante notificaciones de vulnerabilidades técnicas potenciales y relevantes.

d) Una vez identificada las vulnerabilidades técnicas potenciales el IMARPE debe identificar los riesgos asociados y las acciones a ser tomadas en cuenta. Esta acción puede implicar el parchado de sistemas vulnerables y/o la aplicación de otros controles.

e) Dependiendo en que tan urgente sea necesario tratar una vulnerabilidad técnica, la acción a ser tomada en cuenta debe ser llevada a cabo de acuerdo a controles relacionados con la gestión de cambios (véase el inciso 11.5.1) o siguiendo los procedimientos de respuesta ante incidentes en la seguridad de información (véase del inciso 12.2).

f) Si un parche se encuentra disponible, se deben tratar los riesgos asociados con la instalación (los riesgos planteados por la vulnerabilidad deben ser comparados con los riesgos de instalación del parche).

g) Los parches deben ser probados y evaluados antes de que sean instalados con el fin de asegurar que sean efectivos y que no resulten en efectos secundarios que no puedan ser tolerados; si no existe ningún parche disponible, se deberían considerar otros como:

1. Apagar los servicios y capacidades relacionadas con la vulnerabilidad
2. Adaptar o tratar los controles de acceso, por ejemplo los firewall en los bordes de red(véase el inciso 10.4.4)
3. Monitoreo creciente para detectar o prevenir ataques actuales
4. Aumento en la precaución de la vulnerabilidad.

h) Un registro de ingreso debe ser mantenido para todos los procedimientos emprendidos

i) Se debería monitorear y evaluar la gestión de procesos en la vulnerabilidad técnica con el fin asegurar con efectividad y eficiencia

j) Los sistemas en alto riesgo deben ser tratados primero.

12. GESTION DE INCIDENTES EN LA SEGURIDAD DE INFORMACION

12.1 Reportando eventos y debilidades de la seguridad de información

OBJETIVO: Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.

El reporte formal de eventos y los procedimientos de escalada deben estar implementados. Todos los empleados, contratados y terceros deben estar al tanto de los procedimientos para reportar los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales. Se les debe requerir que reporten cualquier evento o debilidad en la seguridad de información, lo más rápido posible, al punto de contacto designado.

12.1.1 Reportando los eventos en la seguridad de información

Todos los empleados nombrados, contratados (CAS) y terceros deben ser prevenidos sobre sus responsabilidades de reportar cualquier evento en la seguridad de información lo más rápido posible. Igualmente, deben ser prevenidos del procedimiento para reportar dicho evento y el punto de contacto. Los procedimientos de reporte deben incluir:

a) Analizar los efectos del incidente y los recursos afectados

Incidentes	Efectos negativos producidos		
	Grave	Moderado	Leve
DoS(Denial of Service)	X		
Código malicioso	X		
Acceso no autorizado	X		
Uso inapropiado		X	
Incidente múltiple	X		
Scanning de puertos			X
Etc.			

Cuadro N° 29: Incidentes

Recursos	Criticidad de los recursos afectados		
	Alta	Media	Baja
Servidor Web	X		
Servidor de Archivos		X	
Servidor de Aplicación	X		
Estaciones de trabajo			X
Conectividad a Internet		X	
Firewall	X		
Compromiso del sistemas	X		
Spam			X
Etc.			

Cuadro N° 30: Criticidad de los recursos

b) Determinar la clasificación del incidente

		Criticidad de los recursos afectados		
		Alta	Media	Baja
Efectos negativos producidos por incidentes potenciales	Grave	Muy Grave	Grave	Moderado
	Moderado	Grave	Moderado	Leve
	Leve	Moderado	Leve	Leve

Cuadro N° 31: Clasificación de Incidentes

c) Definir el tiempo máximo que puede tardarse en comenzar a tratar cada incidente

MUY GRAVE : 10 Minutos

GRAVE : 30 minutos

MODERADO : 2 horas

LEVE : 4 horas

d) Procesos de retroalimentación adecuados para asegurar que dichos eventos reportados de la seguridad de información sean modificados de los resultados después de que el tema haya sido repartido y cerrado.

e) Formularios de reporte de eventos en la seguridad de información, con el fin de apoyar de reporte y para ayudar a la persona que reporta recordar todas las acciones necesarias en caso de un evento.

f) El comportamiento correcto a ser emprendido en caso de un evento en la seguridad de información, por ejemplo:

1. Notar los detalles importantes de eventos: mensajes en la pantalla, conducta extraña, perdida de servicio, equipo o instalaciones, sobrecarga o mal funcionamiento del sistema, errores humanos, no conformidad con políticas o pautas, aberturas en los arreglos de seguridad física, cambios incontrolables en el sistema, mal funcionamiento del software o hardware y violación de acceso)
2. No llevar a cabo ninguna acción por si mismo, pero reportar inmediatamente al punto de contacto.

g) Referencias a un proceso formal disciplinario establecido para tratar con Empleados nombrados, contratados (CAS) y terceros que cometan una abertura en la seguridad.

En ambientes de alto riesgo, se debe proveer una alarma de obligación con el que una persona pueda indicar dichos problemas. Los procedimientos para responder a las alarmas de obligación deben reflejar la situación de alto riego que las alarmas están indicando.

12.1.2 Reportando debilidades en la seguridad de información

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

12.2 Gestión de las mejoras e incidentes en la seguridad de información

OBJETIVO: Asegurar un alcance consistente y efectivo aplicado a la gestión de incidentes en la seguridad de información

Las responsabilidades y procedimientos deben establecerse para maniobrar los eventos y debilidades en la seguridad de información de una manera efectiva una vez que hayan sido reportados. Un proceso de mejora continua debe ser aplicado en respuesta al monitoreo, evaluación y gestión general de los incidentes en la seguridad de información.

Donde se requiera evidencia, esta debe ser recolectada para asegurar el cumplimiento de los requisitos legales.

12.2.1 Responsabilidad y procedimientos

En adición a los reportes de eventos y debilidades en la seguridad de información (véase el inciso 12.1), el monitoreo de los sistemas, alertas y vulnerabilidades (véase el inciso 9.10.2), deben ser utilizados para la detectar los incidentes en la seguridad de información.

a) Los procedimientos deben ser establecidos para maniobrar diferentes tipos de incidentes en la seguridad de información como por ejemplo
    1. Fallas y perdidas de servicio en los sistemas de información
    2. Código malicioso (véase el inciso 9.4.1)
    3. Negación de servicio
    4. Errores Resultantes de datos incompletos o no actualizados
    5. Aperturas en la confidencialidad e integridad
    6. Mal uso de los sistemas de información

b) En adición a los planes de contingencias normales(véase el inciso 13.1.3), los procedimientos también, debe cubrir(véase el inciso 12.2.2)
    1. Análisis e identificación de la causa del incidente
    2. Contención (evitar que el incidente siga produciendo daños)

3. Si es necesario, planteamiento e implementación de acciones correctiva para prevenir la ocurrencia

4. Comunicaciones con los afectados o implicados en recuperarse del incidente.

5. Reportar acciones a la autoridad apropiada.

c) Un registro de auditorias y se debe recolecta evidencia similar(véase el inciso 12.2.3) y resguardar como sea apropiado para:

1. Análisis del problema interno;

2. El uso de evidencia forense en relación con una apertura potencial del contrato, requisitos o en el caso de procedimientos civiles o criminales, como por ejemplo el mal uso del computador o la legislación de protección de datos.

3. Negociaciones para compensaciones por parte de los proveedores de software del servicio.

d) Acción para recuperarse de aperturas de seguridad y controlar formal y cuidadosamente las fallas del sistema que han sido corregidas; los procedimientos deben asegurar:

1. Solo el personal claramente identificado y autorizado están permitidos de acceder a los sistemas y datos on-line (véase también 6.2 para acceso externo)

2. Todas las acciones de emergencia que se realizaron sean documentadas a detalle

3. Las acciones de emergencia sean reportadas a la gerencia y revisados de una manera ordenada.

4. La integridad de los sistemas y controles de negocio son confirmados con un mínimo de retraso.

Los objetivos de la gestión de incidentes en la seguridad de información deben estar acorde con la gerencia y se debe asegurar que los responsables para la gestión entienden las prioridades de la organización para maniobrar dichos incidentes.

12.2.2 Aprendiendo de los incidentes en la seguridad de la información

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

12.2.3 Recolección de evidencia

Los Procesos internos deben ser desarrollados y seguidos cuando se recolecte y presente evidencia para propósitos disciplinarios maniobrados dentro de la organización.

La recolección de la evidencia se puede dar de manera:

1. Información basado en Host : live data collection, ejem. Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la placa de red.

   Forensic duplication, ejem. Backups, archivos copiados recientemente, etc.
2. Información basada en la red: Ejem. Logs de IDSs. Logs de monitoreo, información recolectada mediante sniffers, logs de router. Logs de firewalls, información de servidores de autenticación
3. Otra información. Ejem. Testimonio personal

El proceso de recolección de evidencia debe seguir las siguientes pautas:

a) Registrar información que rodea a la evidencia

- Individuos presentes en el recinto donde se encuentra la evidencia
- Individuos que poseen acceso al recinto donde se encuentra la evidencia
- Los usuarios que pueden utilizar el sistema donde se encuentra la evidencia.

- Ubicación del equipo donde se encuentra la evidencia, dentro del recinto
- Estado del sistema: encendido/apagado
- Fecha y hora del BIOS
- Conexiones de red: Ethernet, MODEM, etc.
- Individuos presentes al momento de efectuar la duplicación de la evidencia
- Numero de serie y modelos de los equipos componentes del equipo.
- Periféricos conectados al equipo

b) Tomar fotografía del entorno de la evidencia

Esto puede efectuarse incluso antes del paso a) y su objetivo es:

- Proteger a la organización y/o a los investigadores ante reclamos por daño a la evidencia
- Regresar el entorno a su condición inicial antes de las actividades forenses
- Registrar visualmente la configuración actual en cuanto a conexiones y a otros periféricos

c) Tomar la evidencia

Se mencionan algunas consideraciones a tener cuenta:

- Capturar información volátil (datos “live”) : conexiones de red. Procesos en ejecución, sesiones logueadas, archivos en uso, configuración de interfaces de red, contenido de memoria
- Generar imagen del disco, de solo lectura
- Obtener copias de los registros de log
- Proteger la evidencia con claves de seguridad o cifrado

d) Registrar la evidencia

- Código de identificador de la evidencia
- Lugar o personas de donde se ha recibido la evidencia
- Descripción breve de la evidencia

- Si se trata de un medio de almacenamiento de datos, descripción de la información que contiene
- Fecha y hora de cuando la evidencia fue recolectada
- Registro de la cadena de custodia: datos de todas las personas que tuvieron la evidencia, fecha y hora de posesión.

e) Rotular todos los medios que serán tomados como evidencia.

- Como mínimo detallar el código de la evidencia en el rotulo
- Guardar la evidencia rotulada en sobre cerrado y firmado. Rotular el sobre.

f) Almacenar toda la evidencia en forma segura

- Protección contra accesos no autorizados
- Protección contra factores nocivos del medio
- Medidas de seguridad en el transporte de la evidencia

g) Realizar las investigaciones en "duplicados de trabajo" de la evidencia original

- Duplicaciones "forensically-sound"
  - No altera ningún dato del medio original
  - Obtiene una copia de cada bit, byte y sector del medio original. Incluso espacios libres no alojados y espacios desperdiciados
  - No contendrá otros datos adicionales a los del medio original
- No es necesario registra las duplicaciones
- Protección contra factores nocivos del medio

h) Realizar copias de seguridad de la evidencia original

- Efectuar las copias lo antes posible, luego de recolectar la evidencia
- Es función de los custodios de la evidencia
- Las copias deben almacenarse en forma segura, al igual que las originales.

i) Realizar revisiones periódicas para garantizar que la evidencia se encuentra correctamente conservada

- Es una función de los custodios de la evidencia

- El objetivo es garantizar que se cumple con el procedimiento de preservación de la evidencia

13. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

13.1 Aspectos de la gestión de continuidad del negocio

OBJETIVO: Minimizar los efectos de las posibles interrupciones de las actividades normales del IMARPE (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia del IMARPE con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) *Notificación / Activación*: Consistente en la detección y determinación del daño y la activación del plan.

b) *Reanudación*: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

c) *Recuperación*: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal del IMARPE y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Responsabilidad

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información (Ver 5.1.2. Asignación de Responsabilidades en Materia de Seguridad de la Información) y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del IMARPE.

- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico institucional para determinar el enfoque global con el que se abordará la continuidad del negocio del IMARPE.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad del negocio del IMARPE.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del IMARPE aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Contingencia y Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatividad de los sistemas de tratamiento de información del IMARPE frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de negocios y/o actividades del IMARPE.
- Asegurar que todos los integrantes del IMARPE comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del IMARPE.
- Elaborar y documentar una estrategia de continuidad del negocio del IMARPE consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad del negocio del IMARPE de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.

- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del IMARPE.
- Proponer las modificaciones a los planes de contingencia.

13.1.1 Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio

El Comité de Contingencia y Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad del negocio del IMARPE.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del IMARPE frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

a) Identificar y priorizar los procesos críticos de los procesos y/o actividades del IMARPE.

b) Asegurar que todos los integrantes del IMARPE comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del IMARPE.

c) Elaborar y documentar una estrategia de continuidad del negocio del IMARPE consecuente con los objetivos y prioridades acordados.

d) Proponer planes de continuidad del negocio del IMARPE de conformidad con la estrategia de continuidad acordada.

e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.

f) Coordinar actualizaciones periódicas de los planes y procesos implementados.

g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del IMARPE.

h) Proponer las modificaciones a los planes de contingencia.

13.1.2 Continuidad del negocio y evaluación de riesgos

Con el fin de establecer un Plan de Continuidad de Negocios del IMARPE se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos y/o actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad Informática, considerando todos los procesos de negocios del IMARPE y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico institucional para determinar el enfoque global con el que se abordará la continuidad del negocio del IMARPE. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Contingencia y Seguridad de la Información a la máxima autoridad del IMARPE para su aprobación.

13.1.3 Redacción e implementación de planes de continuidad que influyen la seguridad de información

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad del negocio del IMARPE. Estos procesos deberán ser propuestos por el Comité de contingencia y Seguridad de la Información. El proceso de planificación de la continuidad del negocio considerará los siguientes puntos:

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.

b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.

c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.

d) Documentar los procedimientos y procesos acordados.

e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.

f) Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

1. Objetivo del plan.
2. Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
3. Procedimientos de divulgación.
4. Requisitos de la seguridad.
5. Procesos específicos para el personal involucrado.
6. Responsabilidades individuales.

g) Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades del IMARPE requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de

personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

13.1.4 Marco de planificación para la continuidad del negocio

Se mantendrá un solo marco para los planes de continuidad del negocio del IMARPE, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deberán ser propuestas por el Comité de Contingencia y Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad del negocio del IMARPE, tendrá en cuenta los siguientes puntos:

a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.

b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del IMARPE y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.

c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del IMARPE o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.

d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del IMARPE.

e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.

f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces.

g) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Los administradores de los planes de contingencia son:

Plan de contingencia	Administrador
Contingencias relacionadas a Siniestros	DE - Director de Administración
Contingencias relacionadas a los Sistemas de Información	DOA - Jefe de la Unidad de Informática
Contingencias relacionadas a los Recursos Humanos	Director de Administración y el jefe de la Unidad de Personal
Plan de Seguridad Física	Director de Administración y el Jefe de la Unidad de Logística e infraestructura

Cuadro N° 32: Administrador del Plan de Contingencia

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

13.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad

Debido a que los planes de continuidad del negocio del IMARPE pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Comité de Contingencia y Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deberán utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).

b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).

c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).

d) Realizar ensayos completos probando que el IMARPE, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del IMARPE se tomarán en cuenta, además, los siguientes mecanismos:

a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del IMARPE en paralelo, con operaciones de recuperación fuera de la Sede Central).

b) Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Los planes de continuidad del negocio del IMARPE serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del IMARPE para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

La periodicidad de revisión de los planes de contingencia (recomendable) es la siguiente:

Plan de contingencia	Revisar cada	Responsable de la revisión
Contingencias relacionadas a Siniestros	cada 6 meses y/o después del evento	Comité de contingencia y seguridad
Contingencias relacionadas a los Sistemas de Información	cada 3 meses y/o después del evento	Comité de contingencia y seguridad
Contingencias relacionadas a los Recursos Humanos	cada 2 meses y/o después del evento	Comité de contingencia y seguridad
Plan de Seguridad Física	cada 3 meses y/o después del evento	Comité de contingencia y seguridad

Cuadro N° 33: Revisión del Plan de Contingencia

Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades del IMARPE aún no reflejadas en dichos planes.

Deberá prestarse atención, especialmente, a los cambios de:

a) Personal.
b) Direcciones o números telefónicos.
c) Estrategia del Organismo.
d) Ubicación, instalaciones y recursos.
e) Legislación.
f) Contratistas, proveedores y clientes críticos.
g) Procesos, o procesos nuevos / eliminados.
h) Tecnologías.
i) Requisitos operacionales.
j) Requisitos de seguridad.
k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
l) Requerimientos de los sitios alternativos.
m) Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Contingencia y Seguridad de la Información para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

14. CUMPLIMIENTO

14.1 Cumplimiento con los requisitos legales

OBJETIVO: Asegurar que no se produzcan incumplimientos legales o transgresiones de la normatividad.

Se recomienda formar un comité que incorpore abogados para validar el cumplimiento de las disposiciones legales.

14.1.1 Identificación de la legislación aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo

se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

Mediante Resolución Ministerial N°. 246-2007-PCM, 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, debiendo ser considerada además en sus respectivos Planes Operativos Informáticos (POI) para su implantación. Finalmente se deja sin efecto la Resolución Ministerial N°. 224-2004-PCM del 23 de julio del 2004, que aprobó la anterior norma técnica peruana NTP-ISO/IEC 17799:2004 EDI. 1era Edición.

14.1.2 Derechos de propiedad intelectual (DPI)

DERECHO DE AUTOR

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los empleados únicamente podrán utilizar material autorizado por el IMARPE.

El IMARPE solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, INDECOPI, es una institución que, dentro de una sociedad en la que los consumidores y proveedores de bienes y servicios asumen el rol que les corresponde como protagonistas del mercado, en su condición de entidad de servicios con marcada preocupación por fomentar una cultura de calidad para lograr la plena satisfacción de sus clientes: la ciudadanía, el empresariado y el estado.

El derecho de autor esta amparado por los siguientes:

- DECRETO LEGISLATIVO 822 - LEY SOBRE EL DERECHO DE AUTOR

- DECISIÓN N° 351: RÉGIMEN COMÚN SOBRE DERECHO DE AUTOR Y DERECHOS CONEXOS

- LEY N° 27861. Ley que exceptúa el pago de derechos de autor por la reproducción de obras para invidentes. Publicado en el Diario Oficial "El Peruano" el 12 de noviembre de 2002.

- LEY Nº 28571. LEY QUE MODIFICA LOS ARTÍCULOS 188º Y 189º DEL DECRETO LEGISLATIVO Nº 822.

  REGLAMENTO DEL REGISTRO NACIONAL DEL DERECHO DE AUTOR Y DERECHOS CONEXOS.

DERECHO DE AUTOR DE SOFTWARE

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El Responsable de Seguridad Informática, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.

b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.

c) Mantener un adecuado registro de activos.

d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.

f) Verificar que sólo se instalen productos con licencia y software autorizado.

g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.

h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.

i) Utilizar herramientas de auditoria adecuadas.

j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

Ley sobre el Derecho de Autor:

"Programa de ordenador (software): Expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un computador ejecute una tarea u obtenga un resultado. La protección del programa de ordenador comprende también la documentación técnica y los manuales de uso." (Decreto Legislativo Nº 822).

Una LICENCIA: todo software divulgado (hecho público) la tiene.

"Autorización o permiso que concede el titular de los derechos (licenciante) al usuario de la obra u otra producción protegida (licenciatario), para utilizarla en una forma determinada y de conformidad con las condiciones convenidas en el contrato de licencia."

Normas de Derecho de Autor:

- Ley de Derecho de Autor (Decreto Legislativo 822).
- Régimen Común sobre Derecho de Autor y Derechos Conexos (Decisión 351 de la Comunidad Andina).
- Guía de la administración de software según Ley N° 28612.
- Inventario de software.
- Inventario de licencias.

Licencias de software libre

- Licencia GPL v.2 (GNU Public License o Licencia Pública GNU) de Free Software Foundation, la más usada por los paquetes de software libre o de código abierto (70% aprox.).
- Para documentación: GNU Free Documentation License (GNU FDL).
- No implican una renuncia total a los derechos de autor. Concede ciertos derechos básicos y reserva todos aquellos no explícitamente concedidos.

Proyecto GNU

Lista de licencias de software libre: http://www.gnu.org/licenses/gpl.html

Open Source Initiative (OSI)

Licencias aprobadas: http://www.opensource.org/licences/

14.1.3 Salvaguarda de los registros de la organización

Los registros críticos del IMARPE se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del IMARPE.

Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoria y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos (ver anexo 6: Control de Registro de Backup).

Las claves criptográficas asociadas con archivos cifrados se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario (Ver inciso 11.3. Controles Criptográficos).

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las

recomendaciones del fabricante.(Ver 11.3.1. Política de Utilización de Controles Criptográficos.)

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para el IMARPE.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información

b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.

c) Mantener un inventario de programas fuentes de información clave.

d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

En particular, se deberán tener presente las siguientes normas:

Ética en el ejercicio de la función publica. LEY Nº 27815 Los Principios, Deberes y Prohibiciones éticos que se establecen en el presente Código de Ética de la Función Pública rigen para los servidores públicos de las entidades de la Administración Pública, de acuerdo a lo establecido en el artículo 4 del presente Código.

Ley sobre el Derecho de Autor:“ Programa de ordenador (software): Expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un computador ejecute una tarea u obtenga un resultado. La protección del programa de ordenador comprende también la documentación técnica y los manuales de uso.” (Decreto Legislativo Nº 822).

14.1.4 Protección de los datos y de la privacidad de la información personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

El IMARPE redactará un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por el IMARPE.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del “Compromiso de Confidencialidad” se deberá advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado (Ver inciso 7. Seguridad del Recursos Humanos).

Son muchos e importantes los cambios y transformaciones que, en el orden jurídico, las TIC´s hacen aparecer. Y, entre otros, debe hacerse mención a la especial importancia que ha adquirido una disciplina como es la relativa a la Protección de Datos y la protección de la intimidad, vinculadas con el Derecho Fundamental a la intimidad que nuestro texto constitucional reconoce en su artículo 2 inciso 6 establece “Que toda persona tiene derecho: a que los

servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"

La protección de los datos personales, tiene por objeto garantizar y proteger en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente su honor e intimidad personal y familiar, de modo que el objeto no se limita sólo a la intimidad, sino que alcanza a la privacidad, un ámbito mucho más amplio que engloba a la intimidad, pero también otros aspectos.

En cuanto al ámbito objetivo de la protección de datos, son tres los elementos que deben ser tenidos en cuenta:

a) El dato de carácter personal, pieza central de la protección de datos, constituido por toda información concerniente a personas físicas identificadas o identificables, de modo que la protección de los datos personales se refiere exclusivamente a la privacidad e intimidad de las personas físicas, pero no de las jurídicas.

Sin embargo, y a pesar de la aparente sencillez del término dato personal, hoy en día podemos encontrar dificultad a la hora de calificar, como dato personal, la dirección de correo electrónico de una persona o sus datos biométricos, lo que obliga a tener en cuenta, adicionalmente, aspectos como la finalidad y tipo de información que dichos datos ofrecen.

b) El fichero de datos personales, respecto del cual recaen parte de las obligaciones que fija la Ley Orgánica de Protección de Datos - LOPD y disposiciones vigentes (entre otras, el Reglamento de Medidas de Seguridad). Es definido como todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso, lo que implica una ordenación de los datos tal, que se permita el acceso a los mismos en atención a algún criterio lógico, como un orden cronológico, alfabético o numérico, pero dicho fichero no tiene porqué estar automatizado.

c) El tratamiento de los datos personales, que no es sino el conjunto de operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

En conclusión, lo esencial para determinar el ámbito objetivo de la LOPD es que nos encontremos ante datos personales, que formen parte o estén en disposición de formar parte de un fichero de datos personales y que los mismos sean objeto de tratamiento, sin que dicho tratamiento deba ir acompañado del adjetivo "automatizado".

Respecto de los elementos subjetivos, hay que decir que las partes de la relación jurídica derivada del tratamiento de los datos personales que necesariamente han de intervenir son fundamentalmente dos. De un lado, el afectado o interesado, que es la persona física titular de los datos que son objeto de tratamiento y, de otro, el responsable del fichero o del tratamiento, que es toda persona física o jurídica, pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.

La Política de Privacidad de la Información Personal siempre ha sido un compromiso importante en una organización, mientras continuamos mejorando la forma en que se recolecta la información personal, ya sea de forma manual, por teléfono, o bien, a través de Internet. Nuestro programa de manejo de la información personal está diseñado para crear y mantener la confianza que existe entre IMARPE y todos aquellos que nos proveen información personal. No lo hacemos sólo porque existan responsabilidades tanto legales como para con el negocio, sino porque es lo correcto.
El recolectar, salvaguardar, así como el adecuado uso de la información personal de la gente tanto interna como externa es uno de los principales valores. Cada uno de nosotros debe de actuar en apego a la Política Global de Privacidad de la Información Personal.

Esta política define el compromiso de proteger la confidencialidad de la Información Personal que se recaba o utiliza en el curso de los negocios. En general se establecerá, mantendrá y supervisará procedimientos comerciales que se apeguen a esta:

- ✓ Se respetará los requerimientos legales que existan en relación con la privacidad de la Información Personal y se compromete a cumplir con todas las leyes correspondientes. IMARPE, en forma ocasional, revisará sus prácticas para recabar, utilizar y revelar Información Personal con el fin de garantizar que se cumplan las leyes y reglamentos.
- ✓ Se avisará y explicará sobre el uso de los requerimientos de la información solicitada; dicho aviso se hará cuando la información personal sea obtenida o cuando ésta sea posteriormente transmitida a terceros. La Información Personal no se utilizará para comercializar un producto o servicio directamente a personas identificables a menos que esta posibilidad se haya aceptado por anticipado.
- ✓ Se avisará las consecuencias de cualquier decisión que tomen las personas respecto a no proporcionar la Información Personal solicitada.
- ✓ Se mantendrá procedimientos que garanticen que la información recabada sobre menores de edad u otras categorías de información sensible, se recopilarán única y exclusivamente con el consentimiento explícito de quien facilite la información, la cual estará protegida contra el mal uso, de acuerdo a lo que la ley señala.
- ✓ Se recabará y utilizará la Información Personal en forma consistente de acuerdo a esta política. Sin embargo, IMARPE podrá decidir retirar cualquier característica identificable de la Información Personal, con el fin de poder obtener resultados estadísticos, históricos, científicos u otros, de acuerdo a lo que la ley señale.
- ✓ Se mantendrá la seguridad de la Información Personal y protegerá su integridad, con un grado de cuidado razonable.

- ✓ Se mantendrá procedimientos consistentes con la ley que se aplique en cada país, con el objeto de que las personas tengan acceso a su Información Personal recabada y, cuando sea necesario, corregirá cualquier información que sea incorrecta o incompleta, cambiará el nivel individual de consentimiento o eliminará la Información Personal.
- ✓ Se requerirá contractualmente que otros que obtengan o proporcionen Información Personal de o para IMARPE, incluyendo las personas dedicadas a prestar servicios de apoyo, como mínimo, adopten y cumplan con los principios y objetivos de esta política.
- ✓ Se publicará procedimientos para responder a las quejas relacionadas con desviaciones potenciales sobre los procedimientos establecidos para proteger la Información Personal.
- ✓ IMARPE, en circunstancias excepcionales, y sólo por requerimiento legal o judicial, recabará, utilizará y/o revelará Información Personal de acuerdo a los procedimientos que no exijan un aviso al interesado (por ejemplo, investigaciones para el cumplimiento de la ley).
- ✓ Se alineará los procesos, políticas, prácticas y guías de Recursos Humanos (información que se recabe o utilice en relación con ex-empleados, empleados actuales o candidatos) para el cumplimiento de esta política.

14.1.5 Prevención en el mal uso de los recursos de tratamiento de información

Los recursos de procesamiento de información del IMARPE se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

En particular, se debe respetar lo dispuesto por las siguientes normas:

Ética en el ejercicio de la función publica. LEY Nº 27815 Los Principios, Deberes y Prohibiciones éticos que se establecen en el presente Código de

Ética de la Función Pública rigen para los servidores públicos de las entidades de la Administración Pública, de acuerdo a lo establecido en el artículo 4 del presente Código.

14.1.6 Regulación en los controles criptográficos

Al utilizar firmas digitales o electrónicas, se deberá considerar lo dispuesto por la Ley Nº 27269, La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Respecto a los controles criptográficos, existe la Resolución del Ministerio del Interior por la que pone en vigor el Reglamento para la criptografía y el servicio central cifrado en el exterior, de 2 de julio de 2002

Se debe obtener asesoramiento antes de transferir a otro país información cifrada o controles criptográficos. Para ello se puede consultar a la Dirección General Migraciones del Perú, Ministerio de Relaciones exteriores, Ministerio de Defensa, a fin de saber si el material exportable requiere algún tratamiento especial.

14.2 Revisiones de la política de seguridad y de la conformidad técnica

OBJETIVO: Asegurar la conformidad de los sistemas con las políticas y normas de seguridad.

Se deben hacer varias revisiones regulares de la seguridad de los sistemas de información.

Estas se deberían atener a las políticas de seguridad apropiadas y se auditara el cumplimiento de las normas de implantación de las seguridad en los sistemas de información y en los controles de seguridad implementados.

14.2.1 Conformidad con la política de seguridad y los estándares

Cada Responsable de Unidad Organizativa (direcciones. Jefaturas y laboratorios), velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas del IMARPE a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Propietarios de información.
d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

14.2.2 Comprobación de la conformidad técnica

El Responsable de Seguridad Informática verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

14.3 Consideraciones sobre auditoria de sistemas

OBJETIVO: Maximizar la efectividad y minimizar las interferencias en el proceso de auditoria del sistema.

Se deberían establecer controles para salvaguardar los sistemas operativos y las herramientas de auditoria durante las auditorias del sistema. También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoria.

14.3.1 Controles de auditoria de sistemas

Cuando se realicen actividades de auditoria que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

a) Acordar con el Área que corresponda los requerimientos de auditoria.

b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoria.

c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoria. Por ejemplo:

- Eliminar archivos transitorios.
- Eliminar entidades ficticias y datos incorporados en archivos maestros.
- Revertir transacciones.
- Revocar privilegios otorgados

d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoria o en su defecto quien sea propuesto por el Comité de Contingencia y Seguridad de la Información completará el siguiente formulario, el cual deberá ser puesto en conocimiento de las áreas involucradas:

Recursos de TI a utilizar en la verificación	
Sistemas de Información	
Base de datos	
Hardware	
Software de auditoria	
Medios magnéticos	
Personal de auditoria	
Interlocutores de las áreas de informática	
Interlocutores de las áreas usuarias	
Conexión a Red	

Cuadro N° 34: Recursos de TI a utilizar

e) Identificar y acordar los requerimientos de procesamiento especial o adicional.

f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:

- Fecha y hora
- Puesto de trabajo.
- Usuario.

- Tipo de acceso.
- Identificación de los datos accedidos.
- Estado previo y posterior.
- Programa y/o función utilizada.

g) Documentar todos los procedimientos de auditoria, requerimientos y responsabilidades.

14.3.2 Protección de las herramientas de auditoria de sistemas

Se protegerá el acceso a los elementos utilizados en las auditorias de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos.

Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido.

Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoria dispuestas.