MINISTERIO DE HACIENDA

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

HOJA DE AUTORIZACIÓN

Preparado por:

Nombre: Ing. Mario Aarón López
Cargo: Coordinador de Seguridad de la Información
Firma:
Fecha: 02/10/23

Revisado por:

Nombre: Ing. Luis Alberto Quezada Arias
Cargo: Subdirector Nacional de Administración Financiera e Innovación
Firma:
Fecha: 09/10/23

Nombre: Ing. Moisés Dubón Carranza
Cargo: Director Nacional de Administración Financiera e Innovación
Firma:
Fecha: 09/10/23

Aprobado por:

Nombre: Lic. Luis Enrique Sánchez Castro
Cargo: Viceministro de Hacienda
Firma:
Fecha: 10/10/23

CONTENIDO

SECCIÓN 1: INTRODUCCIÓN Y ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1.1 INTRODUCCIÓN

"**La seguridad de la información** es la preservación de la confidencialidad, integridad y disponibilidad de la información; en adición, otras propiedades, como la autenticidad, responsabilidad, no-repudiación y fiabilidad pueden estar involucradas". Aunque se puede generar la tendencia que los controles asociados a la seguridad de la información solo están orientados a sistemas de "informática", es importante aclarar que se consideran todos los aspectos relacionados con la información, los medios y los sistemas que la manejan y la soportan.

Los sistemas de información y las redes de las organizaciones están frente a amenazas de un gran número de fuentes, incluyendo fraudes por computadora, espionaje, sabotaje, vandalismo, incendios o inundaciones. Asimismo, causas de daño como códigos maliciosos, "hacking", ataques de denegación de servicios se hacen ahora más frecuentes y sofisticadas.

La seguridad de la información no debe limitarse únicamente a los medios tecnológicos, adicionalmente requiere seguridad en los recursos humanos, seguridad física, seguridad en la gestión de los activos, cumplimiento de la ley y gestionar la continuidad del negocio mediante una gestión apropiada soportada por la política y procedimientos respectivos. Identificar los controles que deben estar implementados requiere una cuidadosa planificación y detalle. La gestión de la seguridad de la información requiere el compromiso y la participación de las máximas autoridades, empleados de la Institución, proveedores, terceras partes, contribuyentes y otros.

Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información (SGSI), provee el modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de la información y los sistemas, para alcanzar los objetivos del negocio, basado en la evaluación del riesgo y los niveles de aceptación del mismo para la Institución, con el fin de gestionar de forma efectiva los riesgos.

Fases del Sistema de Seguridad de la información

De acuerdo a la norma UNE-ISO/IEC 27001:2007, que utiliza el modelo "Planificar –Hacer- Verificar – Actuar", para gestionar el SGSI son las siguientes:

- **Planificar (Establecimiento del SGSI):** Definir la política de seguridad, objetivos, procesos y procedimientos relevantes para gestionar el riesgo y mejorar la seguridad de la información para obtener resultados acordes a los objetivos y políticas de la Institución.

- **Hacer (Implantación y operación):** Implementar y operar la política, controles, procesos y procedimientos del SGSI.

- **Verificar (Seguimiento y revisión del SGSI):** Evaluar y, en su caso, medir el rendimiento de los procesos contra la política, objetivos y la experiencia práctica del SGSI, e informar los resultados a la Dirección para su revisión.

- **Actuar (Mantenimiento y mejora el SGSI):** Adoptar acciones preventivas y correctivas, en función de los resultados de las auditorías internas del SGSI y de la revisión por parte de la Dirección, o de otra información relevante, para lograr la mejora continua del SGSI.

Las fases del PHVA y el diagrama de flujos del modelo se presentan en la Figura 1.

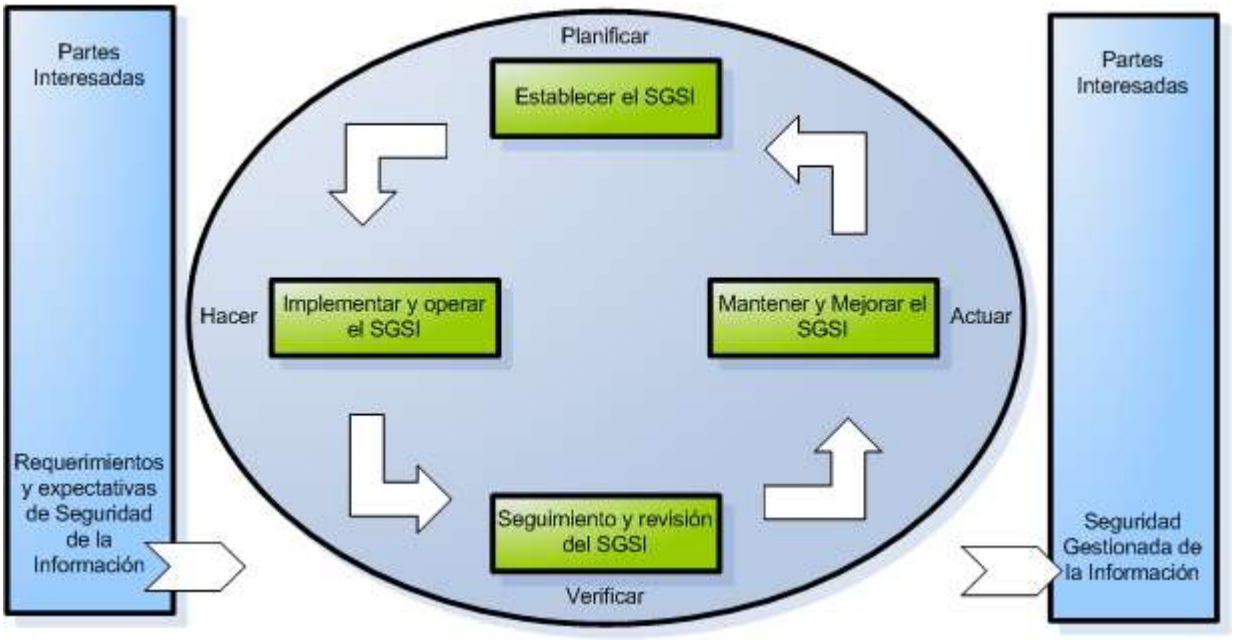

Figura 1. Modelo PHVA (Estándar ISO/IEC 27001)

1.2 OBJETIVOS DEL SGSI

1.2.1 Proteger la información de la Institución y los medios para su tratamiento de forma razonable y continua.
1.2.2 Mantener un modelo de gestión de riesgos de seguridad de la información para su identificación, valoración y tratamiento.
1.2.3 Contribuir a la gestión de la continuidad de los servicios que presta la Institución.
1.2.4 Contribuir al cumplimiento de las normas y legislación en materia de seguridad de la información.

1.3 BASE LEGAL

El presente manual se emite de conformidad a lo establecido en:

1.3.1 Normas Técnicas de Control Interno Especificas del Ministerio de Hacienda.
1.3.2 Manual de Políticas de Control Interno del Ministerio de Hacienda.

1.4 ALCANCE

1.4.1 El SGSI es aplicable a todos los procesos del negocio, la organización, las localidades, los activos de información y tecnología de la Institución.

1.4.2 El cumplimiento del presente Manual es obligatorio para los funcionarios y empleados de las Direcciones o Dependencias que conforman la Institución representadas en el organigrama vigente del Ministerio de Hacienda, excepto la Lotería Nacional de Beneficencia, Fondo Salvadoreño de Estudios de Preinversión y el Instituto Nacional de Pensiones de los Empleados Públicos. Estas disposiciones también serán aplicables a los consultores, contratistas, empleados temporales o terceros que se relacionen con la Institución, en el tratamiento de la información.

1.5 DOMINIOS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

La implantación del SGSI, se hace bajo un enfoque de procesos, para identificar los elementos de entrada y los resultados esperados, a través de la implantación de un conjunto de controles que cubren 11 dominios de seguridad como se especifica en la Figura 3.

Nota: Los requisitos del Sistema de Gestión de Seguridad de la Información definidos en el estándar UNE-ISO/IEC 27001:2007 son compatibles con los requisitos del Sistema de Gestión de la Calidad implantado en la Institución (Ver Sección 11).

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DEL MINISTERIO DE HACIENDA

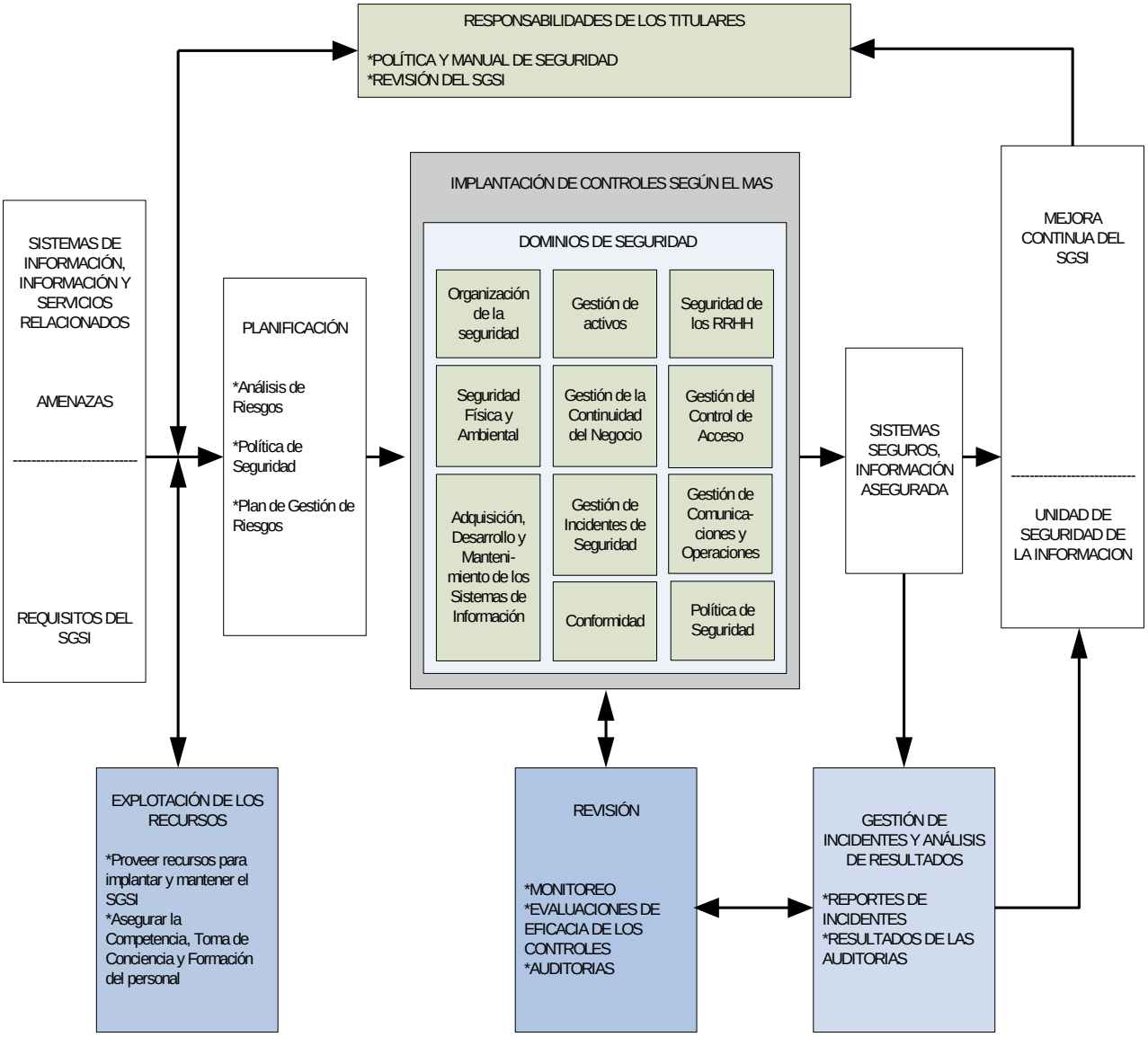

Figura 3. Sistema de Gestión de Seguridad de la Información del Ministerio de Hacienda

SECCIÓN 2: REFERENCIAS

- Norma UNE-ISO/IEC 27001:2007
- Norma UNE-ISO/IEC 27002:2009
- Norma UNE 71502:2004
- Documentación del Sistema de Gestión de Seguridad de la Información (SGSI).

SECCIÓN 3: TERMINOS Y DEFINICIONES

Esta sección comprende una serie de conceptos utilizados en el presente manual y en los documentos relacionados al Sistema de Gestión de Seguridad de la Información, tomando como referencia principal el capítulo 3 Términos y Definiciones de la Norma UNE-ISO/IEC 27001:2007.

3.1 Activo de Información: Recurso del sistema de información o relacionado con éste, necesario para que la Institución funcione correctamente y alcance los objetivos propuestos por su Dirección; en general, algo que tiene valor para la organización.

3.2 AE: Acuerdo Ejecutivo.

3.3 Ambiente de Producción: se refiere al conjunto de recursos y controles destinados a mantener un servicio de tecnologías de la información (por ejemplo: un sitio web o una aplicación del negocio como SAFI, SIDUNEA, SIIP, SIIT, SITEP, entre otros) a disposición de los usuarios

3.4 Amenaza: Una causa potencial de un incidente no deseado, el cual puede producir un daño a un sistema o a la Organización.

3.5 Análisis de Riesgos: Uso sistemático de la información para identificar y estimar las fuentes de riesgo.

3.6 Aplicación del Negocio: Para propósitos de este lineamiento, se refiere a un programa de software creado o desarrollado a la medida, para apoyar o automatizar una función de negocio (contabilidad, tesorería, presupuestos, deuda pública, gestión de tributos, aranceles, entre otros) utilizado por los usuarios finales; cuyo uso no requiere privilegios administrativos. Pueden ser desarrolladas por personal interno, subcontratado, adquiridas directamente del fabricante o recibidos en donación. Ejemplos: SAFI, SIDUNEA, SIIP, SIIT, SIGADE, SIRH, SITEP entre otros.

3.7 Confidencialidad: Propiedad de la información de no estar disponible o no ser revelada a individuos no autorizados, entidades o procesos.

3.8 Control: Medio para gestionar el riesgo, incluyendo p**o**líticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativas, técnicas, de gestión, o legal. El control es también usado como un sinónimo de salvaguarda o contramedida.

3.9 Declaración de Aplicabilidad (DAPL): Declaración documentada que describe los objetivos de los controles y los controles que son relevantes y aplicables al SGSI de la organización. Los objetivos de los controles y los controles son basados en los resultados y las conclusiones de la evaluación de riesgos y el proceso de tratamiento de los riesgos, requisitos legales o regulatorios, obligaciones contractuales y requisitos del negocio de la organización para la seguridad de la información.

3.10 DINAFI: Dirección Nacional de Administración Financiera e Innovación.

3.11 Disponibilidad: Propiedad de la información de ser accesible y utilizable en demanda por entidades autorizadas.

3.12 Evento de Seguridad: Ocurrencia identificada en el estado de un sistema, servicio o red, indicando un posible incumplimiento en la política de seguridad, una falla en las salvaguardas o contramedidas; o una situación previa desconocida que puede ser relevante a la seguridad.

3.13 Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. La gestión de riesgos típicamente incluye la evaluación de riesgos, tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

3.14 Hacking: Acción efectuada por el Hacker.

3.15 Impacto: Consecuencia sobre un activo de la materialización de una amenaza.

3.16 Incidente de Seguridad: Uno o una serie de eventos de seguridad de la información no deseados o inesperados que poseen una probabilidad significativa de comprometer las operaciones del negocio amenazando la seguridad de la información.

3.17 Integridad: Propiedad de salvaguardar la precisión y lo completo de los activos.

3.18 ISO/IEC: Organización Mundial de Estandarización (del griego isos que significa "igual") y la comisión Internacional Electrotécnica (por sus siglas en ingles International Electrotechnical comisión); la cual es una organización que representa una red de institutos de estándares en 156 países. Las siglas preceden a los estándares emitidos por esta organización, ejemplo ISO/IEC 9000; estos estándares se consideran de aplicación internacional.

3.19 MAPO: Manual de Políticas de Control Interno del Ministerio de Hacienda.

3.20 MAS: Manual de Seguridad de la Información del Ministerio de Hacienda.

3.21 No Conformidad: Incumplimiento de un requisito.

3.22 Norma: Es una especificación técnica u otro documento a disposición del público elaborado con la colaboración y el consenso o aprobación general de todas las partes interesadas, basada en resultados consolidados de la ciencia tecnología y experiencia dirigida a promover beneficios óptimos para la comunidad y aprobada por un organismo reconocido a nivel nacional, regional o internacional.

3.23 NTCIE: Normas Técnicas de Control Interno Especificas del Ministerio de Hacienda.

3.24 Período de Conservación de la Información Electrónica: Se refiere a la cantidad de tiempo por el cual la Institución debe mantener la información en formato electrónico de las aplicaciones del negocio, de acuerdo a lo establecido en la normativa legal y técnica vigente aplicable.

3.25 Período de Disponibilidad de la Información Electrónica en Línea: Se refiere a la cantidad de tiempo por el cual se debe mantener la información de las aplicaciones del negocio en las bases de datos para que esté disponible en estas, de forma inmediata, en atención a los requerimientos funcionales de la Dirección o Dependencia.

3.26 Plan de Continuidad del Negocio (PCCN): Es la planificación de todos los recursos necesarios para que se re-establezcan las actividades o servicios que presta una organización a un nivel predeterminado.

3.27 Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

3.28 Registro(s): Documento(s) que presenta(n) resultado(s) obtenido(s) o proporciona(n) evidencia de actividades desempeñadas.

3.29 Recursos para Tratamiento de la Información: Conjunto de elementos disponibles para resolver el manejo, procesamiento, gestión o disposición de la información.

3.30 Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

3.31 Salvaguarda: Acción, procedimiento o dispositivo, físico o lógico que reduce el riesgo.

3.32 SEDE: Secretaria de Estado del Ministerio de Hacienda.

3.33 SGSI: Sistema de Gestión de Seguridad de la Información.

3.34 Soporte(s): Material en cuya superficie se registra información, como el papel, la cinta de vídeo o el disco compacto.

3.35 Unidad de Informática: se refiere a la(s) unidad(es) organizativa(s) que prestan los servicios de tecnologías de la información y comunicaciones para las Direcciones o Dependencias del Ministerio de Hacienda.

3.36 Vulnerabilidad: Debilidad de un activo o grupos de activos que puede ser explotada por una amenaza.

SECCIÓN 4: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.1 REQUISITOS GENERALES

La Institución establecerá, implantará, operará, revisará y mejorará un Sistema de Gestión de Seguridad de la Información de acuerdo con los requisitos establecidos en este Manual para dar cumplimiento a las Políticas de Seguridad contenidas en el capítulo 5 del Manual de Políticas de Control Interno, dentro del contexto de las actividades de negocio de la Institución y los riesgos que ésta enfrenta. Se utilizará para estos fines el proceso de la sección 1.5 basado en modelo PHVA mostrado en la sección 1.1.

4.2 ESTABLECIMIENTO Y GESTIÓN DEL SGSI

4.2.1 Establecimiento del SGSI

La Institución deberá llevar a cabo las siguientes actividades para el establecimiento del SGSI:

a) Definir el alcance del SGSI (ver sección 1.4) en términos de las características de la Institución, como su organización, localización, activos y tecnología.
b) Definir una Política de Seguridad de la Información (Capítulo 5 del MAPO) en términos de las características de la Institución como su organización, localización, activos y tecnología.
c) Adoptar un enfoque hacia la evaluación de los riesgos de la Institución (Capítulo II de NTCIE).
d) Definir una Metodología para el Análisis y Gestión de Riesgos (MAGER) y un procedimiento (PRSN-007 Análisis y Gestión de Riesgos) para la identificación, análisis, evaluación y gestión de los riesgos.
e) Seleccionar los controles para el tratamiento de los riesgos (Con base al estándar UNE-ISO/IEC 27002:2009, ver Anexo 2) los cuales se encuentran detallados a manera de lineamientos en la Sección 9.
f) Gestionar la aprobación ante los Titulares y Directores, Presidente o Jefes de las Unidades Asesoras al Despacho de la propuesta para el manejo de los riesgos residuales.
g) Aprobar la implantación y operación del SGSI (Aprobado por los Titulares en el Capítulo 5 del MAPO y AE Nº 36 del 10 de enero de 2006).
h) Elaborar la Declaración de Aplicabilidad en conformidad con este manual y la norma UNE-ISO/IEC 27002:2009. Este documento deberá ser elaborado por cada Dirección o Dependencia.

4.2.2 Implementación y Operación del SGSI

La Institución deberá llevar a cabo las siguientes actividades para la implementación y operación del SGSI:

a) Cada Dirección o Dependencia formulará un plan de seguridad para el tratamiento de los riesgos, de acuerdo al estándar definido por la DINAFI, que identifique las acciones de la misma, los recursos, responsabilidades y prioridades para el manejo de los riesgos asociados a la seguridad de la información.
b) Cada Dirección o Dependencia implementará el plan de tratamiento de los riesgos en orden de satisfacer los controles identificados.
c) Cada Dirección o Dependencia implementará los controles seleccionados en la Sección 9, para cumplir con los objetivos de estos controles.

d) Cada Dirección o Dependencia definirá como medir la efectividad de los controles seleccionados o grupos de controles y a la vez especificará, como estas medidas serán utilizadas para evaluar la eficiencia y que los resultados producidos sean comparables y reproducibles (ver Sección 4.2.3).
e) La DINAFI impulsará programas de entrenamiento y concientización (ver sección 5.2.2).
f) La DINAFI coordinará operaciones del SGSI.
g) La DINAFI gestionará recursos del SGSI (ver sección 5.2).
h) Cada Dirección o Dependencia implementará procedimientos y otros controles que permitan la detección y respuesta oportuna a los incidentes de seguridad (ver sección 4.2.3)

4.2.3 Supervisión y Revisión del SGSI

Para mantener y mejorar el SGSI mediante el seguimiento, la supervisión y la evaluación del desempeño respecto a la política y los objetivos de la Institución, y notificar los resultados a la Dirección para su revisión, se debe realizar lo siguiente:

a) Cada Dirección o Dependencia ejecutará procedimientos de supervisión y revisión y otros mecanismos de control para:
    1. Detectar errores en la información que se está procesando.
    2. Ayudar a detectar eventos de seguridad y por tanto a prevenir incidentes de seguridad mediante el uso de indicadores.
    3. Identificar debilidades e incidentes en la seguridad de la información de la Dirección o Dependencia.
b) Cada Dirección o Dependencia medirá la eficacia de los controles y verificará que los requisitos de seguridad estén siendo cumplidos.
c) Cada Dirección o Dependencia realizará revisiones periódicas de la efectividad del SGSI tomando en cuenta los resultados de las auditorias de seguridad, incidentes, eficacia de los controles, sugerencias y retroalimentación de todas las partes interesadas.
d) Cada Dirección o Dependencia revisará a intervalos planificados sus análisis de riesgos, los niveles de riesgo residuales, el riesgo aceptado o asumido, tomando en cuenta los cambios en la organización, tecnología, objetivos y procesos de negocio, amenazas identificadas, efectividad de los controles y cambios del entorno legal y reglamentario, de las obligaciones contractuales y del clima social.
e) Cada Dirección o Dependencia actualizará sus planes de seguridad, tomando en cuenta los hallazgos provenientes de las actividades de monitoreo y revisión.
f) Cada Dirección o Dependencia registrará las acciones y eventos que puedan tener impacto en la efectividad y desempeño del SGSI (ver sección 4.3.3).
g) La DINAFI podrá emitir opinión de las revisiones de los análisis de riesgos de cada Dirección o Dependencia.
h) La DINAFI revisará el SGSI de forma regular, para asegurar que el alcance se mantenga adecuado y que las mejoras a los procesos del SGSI sean identificadas (ver sección 7.1).
i) La Unidad de Gestión de la Calidad de SEDE realizará auditorías internas del SGSI a intervalos planificados (ver sección 6).

4.2.4 Mantenimiento y Mejora del SGSI

La Institución deberá llevar a cabo las siguientes actividades para el mantenimiento y mejora del SGSI:

a) Cada Dirección o Dependencia implementará las mejoras identificadas al SGSI.

b) Cada Dirección o Dependencia tomará las acciones preventivas y correctivas de acuerdo a lo establecido en las secciones 8.2 y 8.3.
c) Cada Dirección o Dependencia comunicará las acciones y mejoras a las partes interesadas, en los niveles apropiados de detalle.
d) Cada Dirección o Dependencia asegurará que las mejoras, alcancen los objetivos propuestos.

4.3 DOCUMENTACIÓN DEL SGSI

4.3.1 General

La documentación del SGSI incluye:

a) Alcance del SGSI (ver sección 4.2.1 a)).
b) Política de Seguridad y su objetivo (ver sección 4.2.1 b)).
c) Descripción de la metodología para el análisis y gestión de riesgos (ver sección 4.2.1 c)).
d) Resultado del análisis de riesgo (ver sección 4.2.1 c) a la 4.2.1 g)).
e) Declaración de aplicabilidad.
f) Plan de Seguridad de la Información (ver sección 4.2.2 b)).
g) Procedimientos que aseguren de manera razonable la efectividad de la planeación, operación y control de los procesos de seguridad de la información y que describan como se mide la efectividad de los controles establecidos (ver sección 4.2.3 c)).
h) Registros requeridos en la sección 4.3.3.
i) Procedimientos y controles que soporten el SGSI.

4.3.2 Control de los Documentos

La documentación que sustenta el SGSI, se controla de acuerdo a los requisitos establecidos en la Norma UNE-ISO/IEC 27001:2007.

El control de los documentos está definido en el "PRSN-001 Preparación de Documentos del SGSI" y en el "PRSN-002 Control de Documentos del SGSI", los cuales establecen los aspectos siguientes:

a) Aprobación de los documentos con respecto a su adecuación antes de su emisión.
b) Revisión, actualización y aprobación nuevamente de los documentos en los casos necesarios.
c) Identificación de los cambios y el estado de revisión de los documentos.
d) El proceso para asegurar que las ediciones actualizadas de los documentos que aplican a cada Unidad Organizativa estén en los lugares de uso.
e) Fácil identificación de los documentos y la legibilidad de éstos.
f) Asegurar la disponibilidad, transferencia, almacenamiento y manejo de los documentos de acuerdo a su clasificación.
g) Identificación de los documentos de origen externo.
h) Distribución controlada de los documentos.
i) El mecanismo para evitar el uso de documentos obsoletos.
j) Identificar adecuadamente los documentos, si estos se retienen por cualquier propósito.

4.3.3 Control de los Registros

Con el objeto de proporcionar evidencia de la conformidad de los requisitos, así como de la operación efectiva del SGSI, la Institución ha definido los mecanismos para controlar los registros de seguridad que son requeridos por la Norma UNE-ISO/IEC 27001:2007. Estos se encuentran definidos en el "PRSN-002 Control de Documentos del SGSI", el cual establece los controles para dichos registros, relativo a: la identificación, almacenamiento, protección, recuperación, tiempo de retención y su disposición.

Los registros deben evidenciar la ejecución de los procesos y todos los incidentes significativos de seguridad relacionados al SGSI, como se menciona en la sección 4.2 de este manual.

SECCIÓN 5: RESPONSABILIDADES DE LA ORGANIZACIÓN

5.1 COMPROMISO Y RESPONSABILIDADES DE LA ORGANIZACIÓN

5.1.1 COMPROMISO DE LA ORGANIZACIÓN

5.1.1.1 Titulares

Los Titulares adquieren el compromiso de desarrollar, implantar, mantener y mejorar continuamente el SGSI a través de establecer y aprobar:

a) La política de seguridad de la información
b) Los objetivos del SGSI
c) Los roles y responsabilidades para la seguridad de la información
d) Los recursos para el funcionamiento del SGSI.
e) Los proyectos relacionados a la seguridad de la información.
f) Acuerdo para la designación de la ejecución de las auditorías internas del SGSI.

5.1.2 RESPONSABILIDADES DE LA ORGANIZACIÓN

5.1.2.1 Dirección Nacional de Administración Financiera e Innovación (DINAFI)

Responsable de coordinar el SGSI a través de:

a) Aprobar la documentación relacionada con el funcionamiento del SGSI.
b) Elaborar los documentos normativos del SGSI.
c) Emitir opinión sobre los proyectos, incidentes y fallos relacionados a la seguridad de la Información.
d) Coordinar la planificación e implantación del SGSI.
e) Proporcionar asesoría a los encargados de seguridad de la Institución en la elaboración de procesos relacionados.
f) Gestionar los servicios de asesoría, soporte y mantenimiento de seguridad contratados con especialistas y proveedores.
g) Mantener y publicar la documentación del SGSI.
h) Proporcionar la divulgación de los aspectos relacionados a la seguridad y al SGSI.
i) Revisar anualmente el SGSI una vez éste haya sido implementado.
j) Proporcionar asesoría a los Titulares en materia de seguridad de la información.
k) Definir los criterios para el análisis de riesgos de seguridad de la información y los niveles aceptables del mismo.

5.1.2.2 Directores, Presidente y Jefes de las Unidades Asesoras al Despacho

Responsables de implantar y operar el SGSI, a través de:

a) Cumplir y hacer cumplir lo establecido en los documentos del SGSI.
b) Incorporar y dar seguimiento a las actividades de seguridad en los planes de trabajo de sus Direcciones o Dependencias.
c) Efectuar periódicamente el análisis de riesgo de la información de su Dirección o Dependencia cumpliendo la metodología establecida en el SGSI.
d) Gestionar los recursos para el tratamiento y aceptación de los riesgos de la información.

e) Aprobar la documentación relacionada con la operación del SGSI en su Dirección o Dependencia.
f) Colaborar en la realización de las auditorias al SGSI.
g) Cumplir los requisitos, ejecutar las mejoras y acciones correctivas señaladas en las auditorias.
h) Designar a los "Encargados de Seguridad de la Información" de su Dirección o Dependencia y brindarles el apoyo requerido para desempeñar las funciones asignadas tomando en cuenta los siguientes aspectos:
    1. Conocimiento de los procesos del negocio de la Dirección o Dependencia.
    2. Conocimiento de la información que procesa la Dirección o Dependencia.
    3. Conocimiento de la legislación y marco normativo aplicable a la Dirección o Dependencia.
    4. Conocimiento de las aplicaciones del negocio que se utilizan en la Dirección o Dependencia.
    5. Conocimiento de informática.
    6. Capacidad de negociación, trabajo en equipo y toma de decisiones.
    7. Facilidad de expresión oral y escrita.
i) Sugerir cambios en los lineamientos de seguridad según los riesgos detectados en su Dirección o Dependencia.
j) Velar porque existan mecanismos que permitan la continuidad del negocio de los procesos críticos de su Dirección o Dependencia.

5.1.2.3 Jefes de las Unidades Organizativas

Los Jefes de las Unidades Organizativas tendrán, las responsabilidades siguientes:
a) Cumplir y hacer cumplir lo establecido en los documentos del SGSI.
b) Incorporar y dar seguimiento a las actividades de seguridad en los planes de trabajo de sus Unidades Organizativas.
c) Gestionar con su jefe inmediato los recursos para el tratamiento y aceptación de los riesgos de la información.
d) Revisar o aprobar la documentación relacionada con la operación del SGSI en su Unidad Organizativa.
e) Colaborar en la realización de las auditorias al SGSI.
f) Cumplir los requisitos y ejecutar las mejoras y acciones correctivas señaladas en las auditorias.
g) Definir y someter a aprobación de su jefe inmediato, los proyectos o actividades relacionados con la seguridad de la información.
h) Aplicar las medidas necesarias para gestionar el riesgo asociado a los sistemas de información de sus unidades.
i) Reportar oportunamente las vulnerabilidades e incidentes de seguridad, siguiendo los procedimientos establecidos.
j) Contribuir a la divulgación de la seguridad y el SGSI en sus unidades.
k) Apoyar a los "Encargados de Seguridad de la Información" de su Dirección o Dependencia en el desempeño de las funciones asignadas.
l) Implantar los controles, lineamientos y procedimientos de seguridad establecidos en los documentos del SGSI.

m) Participar cuando sea designado, en la elaboración, implementación, pruebas y mejora del plan de continuidad del negocio de su Dirección o Dependencia cuando su unidad organizativa tenga un alto grado de participación en los procesos críticos.

5.1.2.4 Encargados de Seguridad de la Información

Los Encargados de Seguridad de la Información tendrán, las responsabilidades siguientes:

a) Cumplir y velar por el cumplimiento de lo establecido en los documentos del SGSI.
b) Apoyar y dar seguimiento a las actividades de seguridad en los planes de trabajo de las Unidades Organizativas en su Dirección o Dependencia.
c) Participar en el análisis de riesgo de la información en su Dirección o Dependencia, cumpliendo la metodología establecida en el SGSI.
d) Participar en la revisión de la documentación relacionada con la operación del SGSI en las Unidades Organizativas en su Dirección o Dependencia.
e) Reportar oportunamente las vulnerabilidades e incidentes de seguridad utilizando el mecanismo establecido para la gestión de incidentes de seguridad de la información.
f) Contribuir a la divulgación de la seguridad y el SGSI en su Dirección o Dependencia.
g) Sugerir a la DINAFI cambios en los lineamientos de seguridad según los riesgos detectados en su Dirección o Dependencia.
h) Apoyar la ejecución del análisis de riesgo en sus Direcciones o Dependencias, tomando como referencias los procedimientos y metodología establecida.
i) Apoyar en la implantación los controles, lineamientos y procedimientos de seguridad establecidos en los documentos del SGSI.
j) Apoyar la aplicación de medidas necesarias para gestionar el riesgo asociado a los sistemas de información de sus unidades.
k) Apoyar en la ejecución de las acciones correctivas señaladas por las auditorias en su Dirección o Dependencia.
l) Actuar como enlace entre su Dirección o Dependencia y la DINAFI, en materia de seguridad de la información.
m) Asesorar cuando le sea solicitado, sobre mecanismos que permitan la continuidad del negocio de los procesos críticos de su Dirección o Dependencia.

5.1.2.5 Propietario de la Información

El propietario de la información es el Titular o la(s) persona(s) designada(s), y es en última instancia el responsable de la protección y uso de la información. El propietario de la información tiene la responsabilidad de salvaguardar de forma razonable la confidencialidad, integridad y disponibilidad de la misma, así como asumir la responsabilidad por cualquier acto de negligencia que resulte en la corrupción, destrucción o divulgación de los datos. El propietario decide sobre la clasificación de la información de la cual él es responsable, así como también de actualizar dicha clasificación si el negocio lo considera necesario. Es responsable de asegurar de que estén instalados los controles de seguridad necesarios, que se utilicen los derechos de acceso establecidos, definiendo los requerimientos de seguridad y respaldo por tipo de clasificación, aprobar cualquier actividad de divulgación y definir el criterio de acceso de los usuarios. El propietario de la información aprueba los requerimientos de acceso o puede delegar esta función a las jefaturas de las unidades organizativas. El propietario de los datos delega la responsabilidad del mantenimiento de los mecanismos de protección de los datos, al custodio.

5.1.2.6 Custodio de la Información

El custodio de la información (custodio de los datos en medios físicos y magnéticos) es responsable del almacenamiento y aseguramiento de la información, que le ha sido confiada por el propietario. Cuando se trate de datos en medios magnéticos; este rol es usualmente llevado por la unidad de informática y sus tareas incluyen la realización del respaldo de los datos, la validación periódica de su integridad, restauración, mantener los registros de esta actividad y de cumplir los requerimientos especificados en la política de seguridad de la Institución, estándares y guías referentes a la seguridad de la información y a la protección de los datos.

5.1.2.7 Dueño de Procesos

Son los jefes de las unidades organizativas que tienen la responsabilidad de la coordinación y administración del flujo de trabajo y las actividades en cada etapa de un proceso. Los dueños de proceso deben asegurarse que los procesos bajo su responsabilidad, incluyan las medidas de seguridad adecuada y consistente con la política de seguridad de la información institucional.

5.1.2.8 Personal de Operaciones

Son responsables de implementar los lineamientos, controles, guías y procedimientos de seguridad de la información autorizados por la Institución, en la infraestructura de servidores, clientes y redes de datos, resolver incidentes, aplicar los parches y dar tratamiento a las vulnerabilidades del software. Ante un incidente de ataques a la infraestructura de sistemas y redes, realizan las acciones necesarias para detenerlos y resolverlos utilizando las herramientas y procedimientos adecuados. Son responsables de las actividades de monitoreo de la infraestructura.

5.1.2.9 Especialista y Técnico de Seguridad de la Información de la DINAFI

Asisten en el diseño, implementación, administración y revisión de los lineamientos, controles, estándares, procedimientos y demás documentos de seguridad de la información.

5.1.2.10 Especialista en Ciberseguridad de la DINAFI

Contribuyen a la protección de la infraestructura tecnológica de la Institución a través del análisis de las actividades de las redes de datos, servidores, bases de datos, aplicaciones, sitios web entre otros, a fin de mitigar ciberataques que puedan perjudicar la continuidad de las operaciones en el ámbito digital, mediante la adecuada administración de la seguridad informática y gestión del riesgo.

5.1.2.11 Técnico de Monitoreo de Ciberseguridad de la DINAFI

Contribuyen a la protección de la infraestructura tecnológica de la Institución a través del monitoreo, seguimiento y análisis de las actividades de las redes de datos, servidores, bases de datos, aplicaciones, sitios web entre otros, con el fin de identificar actividades anómalas que puedan indicar incidentes o compromisos de seguridad informática que puedan perjudicar la continuidad de las operaciones.

5.1.2.12 Responsables del Desarrollo de Aplicaciones del Negocio.

Son responsables de implementar los lineamientos, controles y procedimientos autorizados por la Institución, en las aplicaciones del negocio que mantienen o desarrollan.

5.1.2.13 Usuario

Es cualquier individuo que rutinariamente utiliza los datos para realizar tareas relacionadas al trabajo. Sus accesos deben ser autorizados por los propietarios de la información o quienes éstos hayan delegado, además estos accesos, pueden ser restringidos y monitoreados. El usuario debe de tener los niveles de acceso necesarios para realizar sus funciones y es el responsable de seguir los procedimientos operativos de seguridad para asegurar a los demás la confidencialidad, integridad y disponibilidad de los datos. También son responsables de las aplicaciones de usuario final en donde ellos controlen totalmente la seguridad (por ejemplo, hojas de cálculo, procesadores de palabras, entre otros).

5.2 GESTIÓN DE RECURSOS

5.2.1 Provisión de los Recursos

La Institución proveerá los recursos para:

a) Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.
b) Asegurar que los procedimientos de seguridad de la información soporten a los requerimientos del negocio.
c) Identificar los requisitos legales y las obligaciones contractuales de seguridad.
d) Mantener una adecuada seguridad a través de la implementación correcta de los controles.
e) Llevar a cabo revisiones cuando sea necesario y reaccionar apropiadamente a los resultados de las mismas.
f) Cuando se requiera, mejorar la efectividad del SGSI.

5.2.2 Formación, Concientización y Competencia

La Institución para garantizar la formación, concientización y competencia de su personal, realiza lo siguiente:

a) Vela por la competencia del personal que realiza trabajos que afecten la seguridad de la información, considerando para ello los perfiles definidos para cada puesto de trabajo que se encuentran en los manuales de organización.
b) Concientiza al personal sobre la importancia de la seguridad de la información en su puesto de trabajo y de su contribución al logro de los objetivos de seguridad de la información; para lo cual, cuenta con una infraestructura tecnológica que facilita este proceso.
c) Posee registros actualizados del personal, que evidencian la educación, formación, habilidades y experiencia de cada empleado.

SECCIÓN 6: AUDITORIA INTERNA AL SGSI

La Unidad de Gestión de la Calidad de la Dirección General de Administración, es la responsable de realizar las auditorías internas al SGSI.

La Unidad de Seguridad de la Información de la Dirección Nacional de Administración Financiera e Innovación, es la responsable de publicar el informe de auditoría en el Portal del SGSI (https://www.mh.gob.sv/sgsi), comunicando su disponibilidad al Director Nacional de Administración Financiera e Innovación y al Titular de la Dirección o Dependencia.

Las auditorías internas al SGSI se realizarán cumpliendo lo establecido en el procedimiento de calidad “PRO-1.2.2.2 Auditorías Internas del SGC y Verificaciones del SGSI”.

SECCIÓN 7: REVISIÓN POR LA DIRECCIÓN DEL SGSI

7.1 GENERALIDADES

Los Titulares, Directores, Presidente y Jefes de las Unidades Asesoras al Despacho de la Institución, una vez completada la fase de implementación del SGSI (Sección 4.2.2.), con el objeto de asegurarse de la adecuación y efectividad del mismo, revisarán anualmente el Sistema de Gestión de Seguridad de la Información. En la revisión se evaluarán las oportunidades de mejora y las necesidades de realizar cambios al Sistema.

7.2 INFORMACIÓN PARA LA REVISIÓN

La información a considerar para la revisión del SGSI incluye:

a) Los resultados de las auditorias y revisiones del SGSI.
b) La retroalimentación proveniente de terceras partes.
c) Técnicas, productos o procedimientos, utilizados por la Institución para mejorar el desempeño y efectividad del SGSI.
d) Estado de las acciones correctivas y preventivas.
e) Vulnerabilidades o amenazas no tratadas adecuadamente en análisis de riesgos previos.
f) Resultados de las mediciones de efectividad.
g) Acciones de seguimiento de revisiones previas de la Dirección.
h) Cualquier cambio que pueda afectar al SGSI.
i) Recomendaciones de mejora.

7.3 RESULTADOS DE LA REVISIÓN

Los resultados de la revisión del SGSI de la Institución por la alta Dirección, incluyen acciones relativas a:

a) La mejora del SGSI y sus procesos.
b) La actualización de los análisis de riesgos y a los planes para su tratamiento.
c) La modificación de procesos y controles que tienen efecto en la seguridad, de la manera necesaria, para responder a eventos internos o externos que pueden impactar en el SGSI, incluyendo cambios a:
    1. Requisitos del negocio.
    2. Requisitos de seguridad.
    3. Procesos de negocio que tienen efecto a los requerimientos de negocio existente.
    4. Requisitos legales.
    5. Obligaciones contractuales, y
    6. Niveles de riesgos y/o criterios de aceptación de riesgo.
d) Las necesidades de recursos.
e) Las mejoras a la forma en que se mide la efectividad de los controles.

SECCIÓN 8: MEJORA DEL SGSI

8.1 MEJORA CONTINUA

La Institución continuamente mejorará la efectividad del SGSI a través del uso de la política de seguridad de la información, los objetivos de seguridad de la información, los resultados de las auditorias, el análisis de los eventos monitoreados, las acciones correctivas y preventivas y la revisión de la Dirección.

8.2 ACCIONES CORRECTIVAS

La Institución ha definido el proceso a seguir para tomar acciones que eliminen las causas de no conformidades detectadas, con el propósito de evitar su repetición. Se garantiza que las acciones correctivas establecidas y a ejecutar sean apropiadas respecto a la no conformidad determinada.

En el PRSN-006 Acciones Correctivas o Preventivas de Seguridad de la Información, se definen las acciones a seguir para:

a) La revisión por los Jefes de las Unidades Organizativas de las no conformidades que les apliquen, detectadas en auditorias de seguridad.
b) La determinación por Jefes de Unidades Organizativas de causas de no conformidades.
c) El establecimiento de acciones necesarias para impedir que las no conformidades detectadas ocurran nuevamente.
d) La identificación de las acciones correctivas a seguir para corregir las no conformidades y su implantación.
e) El archivo de la hoja de no conformidad, acciones correctivas o preventivas, en la que se registran las acciones tomadas y el seguimiento realizado por cada no conformidad.

8.3 ACCIONES PREVENTIVAS

En el procedimiento PRSN-006 Acciones Correctivas o Preventivas de Seguridad de la Información, se establecen los pasos a seguir para identificar y eliminar las causas de no conformidades potenciales detectadas y prevenir que ocurran. Las acciones realizadas por las Unidades Organizativas para prevenir problemas potenciales, deberían ser apropiadas a las situaciones presentadas, y efectuárseles seguimientos para determinar resultados.

En el PRSN-006 se ha establecido la metodología para:

a) La determinación de no conformidades potenciales y sus posibles causas de ocurrencia.
b) La evaluación de acciones necesarias para prevenir que no conformidades potenciales ocurran.
c) La determinación e implantación de acciones que eviten la realización de la no conformidad potencial detectada.
d) El archivo de las hojas de no conformidad, acciones correctivas o preventivas como registros de seguridad, para respaldar las acciones efectuadas y los resultados obtenidos, y
e) Las acciones preventivas que se toman por no conformidades potenciales, y la verificación de sus resultados.

SECCIÓN 9: LINEAMIENTOS

Esta sección presenta los lineamientos derivados de los controles de la Norma UNE-ISO/IEC 27002:2009, los cuales fueron seleccionados como resultado del análisis de riesgos asociados a los sistemas de información de la Institución y sirven como insumo para la elaboración de la declaración de aplicabilidad; y estarán sujetos a cambios en la norma o reorganizaciones en la Institución.

Es responsabilidad de los funcionarios y empleados, el cumplimiento de estas disposiciones, así como el incluir la seguridad en sus actividades, auxiliándose de los procesos y procedimientos asignados mediante el Sistema de Gestión de Seguridad de la Información (SGSI). Asimismo, reportar las incidencias en materia de seguridad al Encargado de Seguridad de la información de su Dirección o Dependencia.

Los lineamientos contenidos en el presente manual, pueden ser cumplidos a través del Sistema de Gestión de la Calidad de la Institución.

9.1. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

9.1.1 Compromiso con la Seguridad de la Información
La Institución a través de los Titulares brindará apoyo para implantar y mantener la seguridad de la información, destinando los recursos y definiendo funciones y responsabilidades para su sostenimiento.

9.1.2 Autorización de Nuevos Recursos para Tratamiento de la Información
Para la adquisición de recursos destinados al tratamiento de la información, se deberá considerar el cumplimiento de las políticas y lineamientos de seguridad de la Institución.

9.1.3 Divulgación de Información Reservada y Confidencial
La divulgación de información clasificada como reservada o confidencial se realizará conforme a lo establecido en la Ley de Acceso a la Información Pública.

9.1.4 Asesoramiento de Especialistas en Seguridad de la Información
La Institución podrá apoyarse en proveedores o grupos de interés especializados en seguridad de la información, para consultas relacionadas con proyectos, incidentes y fallos de seguridad; cuando no se cuente con los recursos idóneos.

9.1.5 Riesgos Significativos para la Seguridad de la Información Asociados a Partes Externas
Cada Dirección o Dependencia deberá identificar los riesgos para la información y los medios de procesamiento de la misma, a raíz de procesos que involucran a partes externas, debiendo implementar controles apropiados antes de otorgarles acceso.

9.1.6 Requerimientos de Seguridad en las Relaciones con Clientes o Proveedores
Los Jefes de las Unidades Organizativas de cada Dirección o Dependencia, identificarán los requerimientos de seguridad antes de proporcionar acceso a los clientes o proveedores a los activos de información o los recursos de tratamiento de la Institución.

9.1.7 Términos y Condiciones para el Acceso de Terceros
Para regular los accesos de terceros que involucren: procesamiento, comunicación, manejo de la información, medios de procesamiento de la información; o agregar productos o servicios a los medios de

procesamiento de información; los Directores, Presidentes y Jefes de Unidades Asesoras al Despacho deben incorporar los requerimientos de seguridad relevantes en los acuerdos o contratos correspondientes.

9.2. GESTIÓN DE ACTIVOS

9.2.1. Control de Activos

Cada Dirección o Dependencia deberá identificar y llevar un control de los activos importantes relacionados con los procesos, servicios y sistemas de información que los soportan. El control no duplicará innecesariamente los inventarios existentes; para lo cual adoptará el estándar definido por la DINAFI en cuanto a su clasificación y su interrelación con otras Direcciones o Dependencias.

9.2.2. Asignación de Activos

Cada Dirección o Dependencia contará con responsables de los activos de los sistemas de información (incluir en todos procesos o servicios), quienes responderán sobre cualquier cambio, falla, incidente o pérdida de alguna característica de seguridad en cuanto a la información que manejan dichos activos.

9.2.3. Uso de los Activos

La DINAFI definirá lineamientos específicos sobre el uso aceptable de los equipos computacionales, de comunicaciones y el centro de datos.

Las Direcciones o Dependencias definirán las reglas para el uso aceptable de los activos de información bajo su responsabilidad, tomando en cuenta lo establecido en las leyes y el Sistema de Gestión de Seguridad de la Información.

9.2.4. Clasificación de la Información

La información generada por cada Dirección o Dependencia y la confiada a ella por terceros, será clasificada por ésta según lo establece la Ley de Acceso a la Información Pública en el artículo 6, en una de las siguientes categorías:

a) Confidencial: “es aquella información privada en poder del Estado cuyo acceso público se prohíbe por mandato constitucional o legal en razón de un interés personal jurídicamente protegido”; el tipo de información comprendida en esta clasificación se encuentra detallada en el artículo 24 de dicha ley.
b) Reservada: “es aquella información pública cuyo acceso se restringe de manera expresa de conformidad con esta ley, en razón de un interés general durante un período determinado y por causas justificadas”; el tipo de información comprendida en esta clasificación se encuentra detallada en el artículo 19 de dicha ley.
c) Oficiosa: “es aquella información pública que los entes obligados deberán difundir al público en virtud de esta ley sin necesidad de solicitud directa”; el tipo de información comprendida en esta clasificación se encuentra detallada en el artículo 10 de dicha ley.
d) Pública: “es aquella en poder de los entes obligados contenidas en documentos, archivos, datos, bases de datos, comunicaciones y todo tipo de registros que documenten el ejercicio de sus facultades o actividades, que consten en cualquier medio ya sea impreso óptico o electrónico independientemente de su fuente, fecha de elaboración y que no sea confidencial. Dicha información podrá haber sido generada, obtenida, transformada o conservada por éstos a cualquier título”

9.2.5. Marcado y Manejo de la Información

La información confidencial deberá marcarse y será responsabilidad del propietario de la misma tomar las consideraciones correspondientes para asegurar el tratamiento de la misma tomando en cuenta lo establecido en el PRSN-010 “Inventario, Clasificación, Marcado y Manejo de Activos de Información”.

La información reservada deberá marcarse conforme a lo establecido en la Ley de Acceso a la Información Pública (LAIP) y su Reglamento, adicionalmente en caso de considerarse necesario, se podrá marcar esta información según lo establecido en el PRSN-010 “Inventario, Clasificación, Marcado y Manejo de Activos de Información”.

9.3. SEGURIDAD ASOCIADA AL RECURSO HUMANO

9.3.1. Responsabilidades y Perfiles de Puestos

Cada Dirección o Dependencia incluirá en los perfiles de puestos de los funcionarios y empleados, las responsabilidades y descripciones específicas sobre seguridad de la información.

9.3.2. Revisión de Antecedente y Referencias Personales

Las Políticas y procesos de contratación de personal contarán con los controles adecuados en cuanto a la verificación de referencias y antecedentes de los empleados potenciales, cuando estos opten a cargos donde se involucrarán con el manejo de información confidencial o reservada de la Institución.

9.3.3. Términos y Condiciones de Contrataciones

Los contratos a empleados, contratistas y terceros incluirán condiciones que establezcan su responsabilidad y la de la Institución en materia de Seguridad de la Información.

9.3.4. Conocimiento sobre la Documentación del SGSI

La DINAFI realizará tareas de concientización, actualización y divulgación que permitan a los empleados conocer sobre la Seguridad de la Información de la Institución; así como para tener el nivel adecuado de entendimiento de la política, manual, procedimientos y otra documentación del SGSI.

9.3.5. Capacitación en Seguridad de la Información

Cada Dirección o Dependencia será responsable de proveer entrenamiento, capacitación y material de apoyo a sus empleados; con el propósito de lograr un efecto multiplicador de lo dispuesto en el lineamiento 9.3.4 para proteger adecuadamente los activos de información. Adicionalmente, podrá incluir la divulgación de los registros y documentos del SGSI correspondientes a la Dirección o Dependencia.

9.3.6. Cambio o Cese de Funciones

Los jefes de las unidades organizativas están obligados a informar del cambio o cese de funciones de un funcionario o empleado, a los encargados de los Sistemas de Información de la Institución o Encargados de Seguridad de la Dirección o Dependencia, para asignar o revocar los derechos y accesos a la información.

9.3.7. Devolución de Activos

Cada Dirección o Dependencia es responsable de asegurar que los empleados, contratistas y terceros devuelvan los activos de información asignados, una vez cambie o concluya su relación laboral o contractual.

9.3.8. Revocación de Derechos de Acceso

Cada Dirección o Dependencia deberá dar cumplimiento al procedimiento de calidad PRO-6.4.3.1 "Gestión de Accesos" para revocar los derechos de acceso a la información, aplicaciones del negocio, instalaciones de procesamiento y a cualquier otro software o servicio informático; a los funcionarios, empleados, contratistas o terceros al terminar su relación laboral o contractual con la Institución.

9.3.9 Control de los Entrenamientos y Capacitaciones en Temas de Seguridad de la Información.

Toda Dirección o Dependencia que realice actividades de concientización y capacitación en temas de seguridad de la información, remitirá al Departamento de Formación y Desarrollo del Talento Humano del Ministerio de Hacienda, el listado del personal participante.

El Departamento de Formación y Desarrollo del Talento Humano es responsable de mantener actualizados la información de los empleados respecto a actividades de concientización y capacitación en temas de seguridad en que hubiese participado.

9.4. SEGURIDAD FISICA Y AMBIENTAL

9.4.1. Seguridad Física

Cada Dirección o Dependencia debe establecer un perímetro de seguridad (puertas de entrada, paredes, etc.) para proteger las áreas que contengan información y sus recursos de tratamiento.

9.4.2. Control de Acceso Físico a la Información Confidencial o Reservada

El acceso a toda oficina, centro de datos y área de trabajo que contenga información confidencial o reservada debe ser físicamente restringido para limitar el acceso a aquéllos que necesitan la información. Cada Dirección o Dependencia definirá los procedimientos y controles adecuados que proporcionen el detalle del personal autorizado al ingreso a estas áreas.

9.4.3. Protección contra Amenazas Externas y del Ambiente

Cada Dirección o Dependencia solicitará ante la Dirección General de Administración la instalación de protecciones físicas contra incendios, inundaciones, explosiones, disturbios civiles y otras formas de desastres naturales o provocados por el hombre, a los sistemas de información y a la ubicación de los principales activos que los soportan, tomando como base el análisis de riesgo.

9.4.4. Trabajos en Áreas Seguras

Cada Dirección o Dependencia establecerá los controles, procedimientos y protecciones físicas adecuadas, cuando empleados o terceros efectúen trabajos en áreas que contengan información confidencial o reservada.

9.4.5. Ubicación de Sistemas de Cómputo y Equipos de Producción

Los sistemas de cómputo, equipos servidores en producción de los procesos o servicios críticos y equipos centrales de comunicación, serán ubicados físicamente dentro de los centros de datos de la Institución. Se podrán también alojar los equipos servidores de desarrollo y pruebas.

9.4.6. Servicios de Soporte

Cada Dirección o Dependencia solicitará ante la Dirección General de Administración el suministro del mantenimiento de los sistemas de prevención y supresión de incendios, aire acondicionado, sistemas eléctricos, control de humedad y otros sistemas de protección para ambientes computarizados en el centro

de datos de la Institución requeridos.
Los equipos computarizados que alberguen sistemas críticos, computadores personales y estaciones de trabajo estarán equipados con sistemas de alimentación ininterrumpida.

9.4.7. Protección de Equipos Informáticos que contengan Información
Se deberá ubicar o proteger el equipo para reducir las amenazas, peligros ambientales y oportunidades para acceso no-autorizado.

9.4.8. Cables Eléctricos y de Telecomunicaciones
Para efectuar trabajos de instalación y el mantenimiento de infraestructura eléctrica y de telecomunicaciones, los responsables cumplirán las normas y estándares de seguridad vigentes, con el objeto de ser protegido contra la interceptación o daños.

9.4.9. Mantenimiento Preventivo y Correctivo
Las Direcciones o Dependencias gestionarán ante la Dirección Nacional de Administración Financiera e Innovación (DINAFI), las solicitudes de necesidades para el mantenimiento preventivo y correctivo de los equipos críticos y periféricos, que se encuentren fuera del periodo de garantía, que permita la continuidad de las operaciones ejecutadas por los usuarios.

La DINAFI revisará y consolidará las solicitudes de necesidades y remitirá, a la Dirección Financiera el presupuesto estimado para la ejecución de estos mantenimientos.

9.4.10. Seguridad de los Equipos Fuera de las Instalaciones
Cada Dirección o Dependencia garantizará que se atiendan los lineamientos de seguridad emitidos por la DINAFI, cuando por razones de trabajo, se utilicen equipos fuera de las instalaciones de la Institución, que cuenten con la autorización respectiva.

9.4.11. Disposición Final o Reutilización de Equipos
Cada Dirección o Dependencia establecerá procedimientos y controles para garantizar que los equipos que contengan información en sus medios de almacenamiento sean verificados, garantizándose que la información sea eliminada de forma segura (incineración, trituración, borrado o sobre-escritura con software especial o el uso de hardware) antes de su disposición final o reutilización.

9.4.12. Autorización para Salida de Equipos
Los Jefes de las Unidades Organizativas deben autorizar la salida de equipos o cualquiera de sus partes, fuera de las instalaciones de la Institución, cumpliendo los lineamientos establecidos por la Dirección General de Administración en el Manual de Normas para la Administración de los Activos Fijos del Ministerio de Hacienda.

9.5. GESTION DE COMUNICACIONES Y OPERACIONES

9.5.1. Documentación de Sistemas y Procedimientos Operativos
Cada Dirección o Dependencia documentará y mantendrá disponibles para el personal autorizado, los procedimientos operativos que soportan los sistemas de información. En adición los servicios definidos como críticos que incluyan, bases de datos, sistemas operativos, equipos de red y seguridad; deberán contar con la documentación respectiva de sus configuraciones.

9.5.2. Gestión de Cambios

Cada Dirección o Dependencia establecerá los procedimientos necesarios para controlar los cambios en los sistemas de información y sus recursos de tratamiento con base a los definidos por la DINAFI. Los datos de producción serán modificados sólo por el personal autorizado de acuerdo con dichos procedimientos.

9.5.3. Separación de Funciones

Los responsables de definir los requerimientos de los sistemas y los de ambientes de producción, deben implementar controles que incluyan la separación de funciones incompatibles tales como autorización, ejecución, registro, custodia y control; a fin de reducir la posibilidad de que se produzcan modificaciones no autorizadas o el uso indebido de los activos de información de la organización.

9.5.4. Separación de Ambientes de Desarrollo, Prueba y Producción

Cada Dirección o Dependencia deberá separar y utilizar de forma eficiente, los recursos de desarrollo, prueba y producción relacionados a los sistemas de información. Los administradores de Sistemas Operativos, Bases de Datos, Equipos de Comunicaciones, Servidores de Aplicaciones y de Estaciones Clientes, no deben tener instalados compiladores o herramientas de desarrollo en sus estaciones de trabajo ni en los servidores que administran, a menos que esté debidamente autorizado, de forma escrita, por el jefe de la unidad de informática de la Dirección o Dependencia.

Los usuarios que participen en el proceso de pruebas de aplicaciones del negocio deben utilizar una cuenta de usuario distinta a la que tenga asignada en el ambiente de producción.

No se deberán utilizar datos de producción en ambientes de desarrollo y cuando éstos sean confidenciales o reservados no podrán ser utilizados en ambiente de prueba.

9.5.5. Gestión de la Capacidad

El uso de los componentes críticos para el tratamiento de la información en las aplicaciones del negocio clasificadas como críticas o vitales será constantemente monitoreado y se tomarán como base los resultados de esta tarea para hacer proyecciones oportunas de futuro crecimiento, para asegurar el desempeño de los sistemas de información automatizados.

9.5.6. Aceptación de Sistemas y Aplicaciones de Producción

Los responsables del desarrollo de las aplicaciones del negocio deben obtener por parte del solicitante, evidencia de la aceptación de los nuevos sistemas y aplicaciones o modificaciones mayores, antes de que éstas se desplieguen en producción.

9.5.7. Código Malicioso

Los jefes de las unidades de informática de cada Dirección o Dependencia deben establecer controles, procedimientos y mecanismos de divulgación o concientización para prevenir, detectar y recuperarse del código malicioso.

9.5.8. Configuración de Software y Controles de Seguridad de Equipos Cliente

La Unidad de Informática de cada Dirección o Dependencia debe asegurarse que las estaciones clientes y computadoras portátiles, antes de que sean entregados al usuario final, cuentan con las medidas de seguridad establecidas en los Documentos Normativos del SGSI.

9.5.9. Respaldo de la Información en Medios Magnéticos
Los responsables de efectuar los respaldos del software y de la información de cada Dirección o Dependencia, deben llevarlos a cabo de acuerdo a los lineamientos específicos establecidos por la DINAFI para tal efecto y realizar pruebas a los mismos de forma regular.

9.5.10. Controles de Red de Datos
La DINAFI definirá y establecerá los controles y procedimientos de gestión de la red de datos y sus accesos, con el fin de protegerlas contra amenazas y mantener el funcionamiento y operación de los sistemas que las utilizan, incluyendo la información en tránsito.

9.5.11. Seguridad en los Servicios de Red de Datos
La DINAFI definirá y establecerá controles, estándares de seguridad y niveles de servicio a incluir en los contratos relacionados con la utilización o entrega de los servicios de red, a través de redes de terceros y donde sea aplicable a las redes propias de la Institución.

9.5.12. Eliminación de los Soportes
Cada Dirección o Dependencia eliminará de forma segura la información contenida en soportes de almacenamiento de datos (cintas, discos, memorias USB, discos duros removibles, discos duros USB, discos Blu-ray, DVD, CD, diskettes, memoria SD, etc.) cuando sean dados de baja, pudiendo aplicar los criterios de referencia publicados en el SGSI, con el objeto de evitar la divulgación o el uso no autorizado de la información contenida en los mismos.

9.5.13. Utilización de la Información
Cada Dirección o Dependencia establecerá los controles y procedimientos para la utilización y almacenamiento de la información en medio físico o magnético, con el objeto de protegerla del mal uso o divulgación y acceso no autorizados.

9.5.14. Intercambio de Información y Software
Cada Dirección o Dependencia establecerá controles que regulen el intercambio de información o software a través de cualquier medio de comunicación de acuerdo a las disposiciones legales y técnicas vigentes, sea este interno o con entidades externas. Para el caso de intercambio con entidades externas; a través de medios electrónicos, se debe establecer por escrito un acuerdo o convenio de intercambio de información. Para gestionar la interconexión, se realizará de acuerdo a lo establecido en los procedimientos de la Unidad de Redes de la DINAFI y de la División de Modernización de la Dirección General de Aduanas según el caso.

9.5.15. Soportes Físicos en Tránsito
Cada Dirección o Dependencia establecerá los controles de seguridad para el transporte de los soportes de información.

Para el caso del transporte de medias de respaldo de los equipos servidores del centro de datos se regirán por los Lineamientos Específicos de Seguridad de la Información para la Gestión de Respaldos de Información del Ministerio de Hacienda.

9.5.16. Mensajería Electrónica
La DINAFI establecerá los Lineamientos Específicos de Seguridad para el Servicio de Correo Electrónico del Ministerio de Hacienda, Acceso y Uso del Servicio de Internet del Ministerio de Hacienda que

contenga los controles para la protección de la información contenida, relacionada o transmitida por medios electrónicos.

9.5.17. Seguridad en la Interconexión de Sistemas de Información de Negocios
Cada Dirección o Dependencia desarrollará controles para proteger la información asociada con la interconexión de los sistemas de información de negocios.

9.5.18. Comercio Electrónico
Las aplicaciones de negocio del Ministerio de Hacienda que permitan el intercambio de información o registro de transacciones en línea con terceros a través del Internet, deben implementar controles orientados a proteger la confidencialidad de información sensible en tránsito y la autenticidad del sitio web de la Institución.

9.5.19. Pagos a Empleados y Terceros
La Institución, en su relación con proveedores y empleados que involucren el pago de bienes, servicios, remuneraciones u otros y sea necesario efectuarlos a través de medios electrónicos o manuales, garantizará que el medio y los mecanismos para el manejo de la información, cuenten con las características de seguridad razonables para evitar comprometer dicha información.

9.5.20. Información Disponible al Público
Los responsables de administrar los equipos o medios que contengan información disponible al público (oficiosa y pública), implantarán los controles para proteger la información ante modificaciones no autorizadas.

9.5.21. Registros o Huellas de Auditoria
Las aplicaciones del negocio que manejen información reservada o confidencial, aplicaciones del negocio clasificadas como críticas o vitales, Directorios de usuarios y los componentes críticos de infraestructura contarán con registros que capten las actividades de los usuarios, administradores y operadores de toda consulta, adición, cambio o eliminación de la información relacionada a las transacciones del negocio.

9.5.22. Protección de los Registros o Huellas de Auditoría
Los registros o huellas de auditoría deben protegerse para evitar su modificación y sólo podrán ser accedidos por personal autorizado.

9.5.23. Registros de Fallas
Cada Dirección o Dependencia identificará y registrará las fallas de los componentes críticos de infraestructura asociadas a las aplicaciones del negocio clasificadas como críticas, vitales y aquellas que manejan información reservada o confidencial con el objeto de tomar las acciones apropiadas.

9.5.24. Sincronización del Reloj
Los equipos computacionales, de comunicación de datos y otros componentes de las aplicaciones del negocio y los componentes críticos de infraestructura de la Institución, deben sincronizarse con la hora del equipo central de comunicación definido por la DINAFI.

9.5.25 Política de Retención de Información Electrónica
Cada Dirección o Dependencia determinará el período de conservación de la información electrónica en las bases de datos de las aplicaciones del negocio bajo su responsabilidad en ambiente de producción, de

acuerdo a la normativa legal y técnica vigente que aplique a esa información y conforme a lo establecido en los "Lineamientos Específicos para la Gestión de Respaldos de Información en Medios Magnéticos y Definición de Periodos de Retención de Información Electrónica del Ministerio de Hacienda" (LES-005).

9.5.26 Política de Disponibilidad en Línea de la Información Electrónica
Cada Dirección o Dependencia determinará el período de disponibilidad en línea de la información electrónica en las bases de datos de las aplicaciones del negocio bajo su responsabilidad, de acuerdo a sus necesidades y considerando los costos económicos para este tipo de servicio y conforme a lo establecido en los "Lineamientos Específicos para la Gestión de Respaldos de Información en Medios Magnéticos y Definición de Periodos de Retención de Información Electrónica del Ministerio de Hacienda" (LES-005).

9.5.27 Eliminación de Información Electrónica con Periodo de Conservación Vencido
Cada Dirección o Dependencia que tenga información en las bases de datos de las aplicaciones del negocio en ambiente de producción y cuyo periodo de conservación de la información electrónica haya vencido, autorizará la eliminación de ésta.

9.6. CONTROL DE ACCESOS

9.6.1. Política de Control de Acceso
Cada Dirección o Dependencia controlará el acceso a su información y recursos de tratamiento, basados en los lineamientos de control de acceso emitidos por la DINAFI.

9.6.2. Registro de Usuarios
Cada Dirección o Dependencia debe establecer un procedimiento formal de registro y desactivación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información de acuerdo a los lineamientos de control de acceso emitidos por la DINAFI.

9.6.3. Gestión de Privilegios
La asignación y el uso de privilegios deben estar restringidos y controlados de acuerdo a los lineamientos de control de acceso emitidos por la DINAFI.

9.6.4. Gestión de Contraseñas de Usuario
La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal de acuerdo a los lineamientos de control de acceso emitidos por la DINAFI.

9.6.5. Directorios de Usuarios
La DINAFI definirá el estándar para el servicio de directorio que contengan a los usuarios y recursos asociados de la Institución.

9.6.6. Revisión de los Derechos de Acceso de Usuario
Cada Dirección o Dependencia semestralmente efectuará la revisión de los derechos de acceso de los usuarios a la red, a las aplicaciones del negocio clasificadas como críticas o vitales y aquellas aplicaciones del negocio que manejan información confidencial o reservada, a efecto de revocar estos derechos después de 60 días o más de inactividad sin justificación.

9.6.7. Uso y Estructura de las Contraseñas

Las contraseñas son estrictamente personales e intransferibles y es responsabilidad directa del usuario los incidentes de seguridad que puedan ser causados por descuido, divulgación o mala utilización de ésta. Adicionalmente, los usuarios seguirán los lineamientos de control de acceso emitidos por la DINAFI para su creación y buenas prácticas de seguridad.

9.6.8. Computadores Desatendidos

Los usuarios deben activar el protector de pantalla protegido por contraseña, cuando vayan a dejar sus estaciones de trabajo desatendidas.

9.6.9. Uso de los Servicios de Red

Cada Dirección o Dependencia atenderá los lineamientos de red establecidos por la DINAFI para el uso de los servicios de red de la Institución; los cuales serán asignados conforme a las funciones de los puestos de trabajo de los empleados, contratos o convenios suscritos con terceros.

9.6.10. Autenticación de Conexiones Externas

Los administradores de la red de datos deben aplicar mecanismos que aseguren la autenticación de los usuarios remotos que acceden a la red interna de la Institución, excepto el acceso externo a información pública u oficiosa dispuesta en los sitios Web de la Institución destinada para el público en general, ubicando los equipos de esta última en una zona de seguridad separada de la red interna.

9.6.11. Diagnostico Remoto y Protección de los Puertos de Configuración

El acceso a los puertos de diagnóstico y de configuración se controlará de conformidad a los lineamientos de red definidos por la DINAFI.

9.6.12. Segregación de Redes de Datos

Los administradores de redes de la Institución deben segregar en subredes, los grupos de servicios de información, usuarios y sistemas de información.

9.6.13. Control de Conexiones a la Red

Los administradores de redes deben limitar el acceso de los usuarios para conectarse a la red, de acuerdo a los Lineamientos de Seguridad de la Información para el Control de Acceso a la Información del Ministerio de Hacienda, los Lineamientos de Seguridad de la Información para los Servicios y Gestión de Accesos a la Red de Datos del Ministerio de Hacienda emitidos por la DINAFI y a los requisitos de las aplicaciones del negocio.

9.6.14. Procedimientos para Inicio de Sesión

El acceso a los sistemas operativos se debe controlar por medio de un procedimiento seguro de inicio de sesión, en cumplimiento a lo definido en los lineamientos de control de accesos.

9.6.15. Identificación y Autenticación de Usuario

Todos los identificadores de usuario se construirán de conformidad con los lineamientos de control de acceso emitidos por la DINAFI, eligiendo una técnica adecuada de autenticación para confirmar la identidad solicitada al usuario.

9.6.16. Uso de los Recursos del Sistema

Se debe restringir y controlar rigurosamente el uso de programas y utilidades que puedan ser capaces de

invalidar los controles del sistema y de las aplicaciones del negocio de acuerdo a los lineamientos de control de acceso emitidos por la DINAFI.

9.6.17. Software Estándar en Estaciones de Trabajo
Las estaciones de trabajo de cada Dirección o Dependencia contarán con software definido como estándar para efectos de trabajo, de conformidad a los lineamientos establecidos por éstas.

9.6.18. Desinstalación de Herramientas
Los usuarios no desinstalarán las herramientas de seguridad, administración y control de inventarios de las estaciones de trabajo asignadas.

9.6.19. Instalación o Desinstalación de Software
La instalación o desinstalación software en los equipos de computación debe ser realizado únicamente por el personal informático autorizado, atendiendo los procedimientos establecidos para tal fin.

9.6.20. Computadores Portátiles con Información Reservada o Confidencial
Los usuarios responsables de computadores portátiles que contengan información reservada o confidencial, se apoyarán en las unidades de informática de la Dirección o Dependencia para garantizar que dichos equipos cuenten con medidas de seguridad, por ejemplo: contraseña de arranque, usuario y contraseña de sistema operativo.

9.7. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

9.7.1. Análisis y Especificación de los Requisitos de Seguridad
Los propietarios de la información o las personas que designen para definir los requerimientos de las aplicaciones del negocio, deben incluir los controles de seguridad a ser implementados, tanto para los sistemas de información nuevos o para mejoras a los mismos, atendiendo los lineamientos para el desarrollo, mantenimiento o adquisición de aplicaciones del negocio emitidos por la DINAFI.

9.7.2. Validación de los Datos de Entrada
La introducción de datos en las aplicaciones del negocio debe validarse para garantizar que dichos datos son correctos y adecuados conforme al proceso de negocio que soportan. Los propietarios de la información o las personas que designen son responsables de definir estas validaciones.

9.7.3. Control del Procesamiento Interno
Los propietarios de la información o las personas que designen para definir requerimientos de las aplicaciones del negocio, deben definir los procesos críticos para incorporar comprobaciones de validación que detecten cualquier corrupción de la información, debido a errores de procesamiento o actos intencionados.

9.7.4. Integridad de los Mensajes
Se deben identificar los requisitos para garantizar la autenticidad y proteger la integridad de los mensajes en los servicios web y se deben identificar e implantar los controles adecuados.

9.7.5. Validación de los Datos de Salida
Los propietarios de la información o las personas que designen para definir requerimientos de las aplicaciones del negocio, deben especificar los controles para validar que la información almacenada es correcta y adecuada a las circunstancias.

9.7.6. Control de las Aplicaciones del Negocio en Producción
Los responsables del despliegue de las aplicaciones del negocio en ambiente de producción, deben tener implantados procedimientos para controlar la instalación de éstas en los sistemas operativos.

9.7.7. Falla de las Aplicaciones del Negocio
Los responsables del desarrollo de las aplicaciones del negocio deben asegurar que cuando éstas fallen y no produzca los resultados esperados, proporcione un mensaje de error comprensible o alguna otra indicación de falla como respuesta al usuario.

9.7.8. Retroalimentación de las Aplicaciones del Negocio al Usuario
Los responsables del desarrollo las aplicaciones del negocio deben asegurar que cuando ejecute en una transacción, ésta dará respuesta cuando amerite según los requerimientos del solicitante, indicando si se llevó a cabo la solicitud.

9.7.9. Prueba de las Aplicaciones del Negocio
Todas las aplicaciones del negocio adquiridas o desarrolladas internamente, pasarán por un proceso de pruebas documentado que garantice la calidad y seguridad de las mismas.

9.7.10. Instalación de las Aplicaciones del Negocio en Producción
Las aplicaciones del negocio serán trasladadas al ambiente de producción por personal de tecnología autorizado e independiente a las áreas de desarrollo.

9.7.11. Protección de los Datos de Prueba del Sistema
Los datos de prueba deben seleccionarse cuidadosamente, estar protegidos y controlados. Adicionalmente, no deben efectuarse pruebas de software directamente en producción.

9.7.12. Control de Acceso a Código Fuente de los Programas
Los Responsables del Desarrollo de Aplicaciones del Negocio de cada Dirección o Dependencia restringirán el acceso a los códigos fuentes de los programas y aplicaciones utilizados en sistemas de información automatizados, de acuerdo a los lineamientos de control de acceso emitidos por la DINAFI.

9.7.13. Procedimiento de Control de Cambios
Cada Dirección o Dependencia empleará procedimientos de control de cambios, para autorizar y desplegar las modificaciones al software y aplicaciones del negocio en el ambiente de producción.

9.7.14. Control de Cambios del Código Fuente
Para controlar los cambios de las aplicaciones del negocio en producción, se debe emplear un sistema de control de versiones del código fuente.

9.7.15. Revisión Técnica de las Aplicaciones tras Efectuar Cambios en el Sistema Operativo
Cada Dirección o Dependencia, debe revisar y probar las aplicaciones del negocio críticas, cuando se apliquen cambios mayores a los sistemas operativos de los ambientes de producción, para garantizar que no existen efectos adversos en las operaciones o en la seguridad.

9.7.16. Desarrollo de Software por Terceros
La Dirección o Dependencia solicitante de proyectos de desarrollo de software por terceros, debe incluir

en los requerimientos de contratación adicionalmente a las especificaciones técnicas, los siguientes aspectos:

a) definiciones de arreglos de licencia
b) propiedad intelectual
c) cumplimiento de las políticas de seguridad de la información del Ministerio de Hacienda
d) seguridad y calidad del software desarrollado
e) acuerdos de garantías
f) entrega del código fuente
g) requerimientos de pruebas y puesta en producción

9.7.17. Control de Vulnerabilidades de Software

El personal responsable de administrar equipos de computación, de comunicación de datos y el software desplegado en éstos, deben revisar de forma periódica y oportuna, la información sobre vulnerabilidades de sistemas operativos y aplicaciones de software en operación utilizadas en su Dirección o Dependencia y aplicar las medidas adecuadas para mitigar el riesgo asociado.

9.8. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

9.8.1. Notificación de los Eventos de Seguridad de la Información

Los empleados, contratistas y usuarios de las aplicaciones del negocio, software en general y servicios de información de la Institución, deben reportar oportunamente los eventos de seguridad de la información a través del sistema de mesa de servicios, proporcionado por la DINAFI.

9.8.2. Responsabilidades y Procedimientos de Gestión de Incidentes de Seguridad

Cada Dirección o Dependencia definirá procedimientos de gestión, que dicten los pasos a seguir para corregir y prevenir incidentes de seguridad de la información, mediante una respuesta rápida, efectiva y ordenada, de acuerdo a los lineamientos para la gestión de incidentes de seguridad de la información emitidos por la DINAFI.

9.8.3. Base de Conocimiento sobre Incidentes de Seguridad

Se establecerá como parte del sistema de mesa de servicios, una base de conocimientos para facilitar el análisis, aprendizaje y prevención de los incidentes de seguridad.

9.9. GESTION DE CONTINUIDAD DEL NEGOCIO

9.9.1. Seguridad de la información en el Proceso de Continuidad del Negocio

Cada Dirección o Dependencia debe desarrollar y mantener un proceso para la continuidad del negocio, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio basado en el modelo proporcionado por la DINAFI.

9.9.2. Continuidad del Negocio y Evaluación de Riesgos

Cada Dirección o Dependencia debe deben identificar los eventos que puedan causar interrupciones en sus procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones basado en el modelo proporcionado por la DINAFI.

9.9.3. Desarrollo e Implantación de Planes de Continuidad del Negocio que Incluyan la Seguridad de la Información

Las Direcciones o Dependencias deben desarrollar e implantar planes para mantener o restaurar las operaciones y garantizar su disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o fallo en los procesos de negocio críticos.

9.9.4. Pruebas, Mantenimiento y Reevaluación de los Planes de Continuidad del Negocio
Las Direcciones o Dependencias deben probar y actualizar al menos una vez al año, los planes de continuidad del negocio para asegurar que están al día y son efectivos. Las pruebas deben ser planificadas y documentadas conforme al modelo proporcionado por la DINAFI, y se deberá informar a los Titulares sobre los resultados de éstas.

9.10. CONFORMIDAD

9.10.1. Identificación de la Legislación Aplicable
Las Direcciones o Dependencias deben identificar las disposiciones legales que les aplican y gestionar su cumplimiento considerando implementar procedimientos registrados en el Sistema de Gestión de la Calidad o cambios en los Documentos del SGSI para tal efecto.

9.10.2. Registro de Software de Desarrollo Interno y Derechos de Autor
Cada Dirección o Dependencia será responsable de gestionar el registro en la entidad competente del software desarrollado para aplicaciones del negocio clasificadas como críticas o vitales, a efectos de garantizar los derechos de propiedad intelectual y auditoria a nombre de la Institución.

9.10.3. Cumplimiento de las Políticas y Normas de Seguridad
Los Directores, Presidente, Jefes de Unidades Asesoras al Despacho deben apoyar para el cumplimiento de lo establecido en el Sistema de Gestión de Seguridad de la Información dentro de su área de responsabilidad.

9.10.4. Protección de Herramientas de Auditoría
El acceso a las herramientas de auditoría de los sistemas de información debe estar protegido por los responsables de éstos, para evitar cualquier posible peligro o uso indebido.

SECCIÓN 10: INCUMPLIMIENTO A LAS POLÍTICAS Y LINEAMIENTOS

Los empleados y funcionarios que incumplan las políticas y lineamientos de seguridad de la información adoptada por esta Institución, estarán sujetos a acciones disciplinarias establecidas en las disposiciones legales y técnicas vigentes.

SECCIÓN 11: ANEXOS

ANEXO 1

CORRESPONDENCIA ENTRE LOS CONTROLES DEL ESTÁNDAR UNE-ISO/IEC 27002:2009 CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LOS LINEAMIENTOS DEL MANUAL DE SEGURIDAD DE LA INFORMACION DEL MINISTERIO DE HACIENDA

UNE-ISO/IEC 27002:2009		MAS	
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**6**	**9.1**	**ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN**
Organización Interna	**6.1**		
Comité de Gestión de Seguridad de la Información	6.1.1	9.1.1	Compromiso con la Seguridad de la Información
Coordinación de la Seguridad de la Información	6.1.2		SECCIÓN 5: Responsabilidades de la Organización
Asignación de Responsabilidades Relativas a la Seguridad de la Información	6.1.3		
Proceso de Autorización de Recursos para el Procesado de la Información	6.1.4	9.1.2	Autorización de Nuevos Recursos para Tratamiento de la Información
Acuerdos de Confidencialidad	6.1.5	9.1.3	Divulgación de Información y Acta Notarial de Confidencialidad
Contacto con Grupos de Especial Interés	6.1.7	9.1.4	Asesoramiento de Especialistas en Seguridad de la Información
Revisión Independiente de la Seguridad de la Información	6.1.8		SECCIÓN 6: Auditoría Interna al SGSI SECCION 7: Revisión por la Dirección del SGSI
Terceros	**6.2**		
Identificación de los Riesgos Derivados del Acceso a Terceros	6.2.1	9.1.5	Riesgos Significativos para la Seguridad de la Información Asociados a Partes Externas
Tratamiento de la Seguridad en Relación con los Clientes	6.2.2	9.1.6	Requerimientos de Seguridad en las Relaciones con Clientes o Proveedores
Tratamiento de la Seguridad en Contratos con Terceros	6.2.3	9.1.7	Términos y Condiciones para el Acceso de Terceros
GESTIÓN DE ACTIVOS	**7**	**9.2**	**GESTIÓN DE ACTIVOS**
Responsabilidad sobre los Activos	**7.1**		
Inventario de Activos	7.1.1	9.2.1	Control de Activos
Propiedad de los Activos	7.1.2	9.2.2	Asignación de Activos
Uso Aceptable de los Activos	7.1.3	9.2.3	Uso de los Activos
Clasificación de la Información	**7.2**		
Directrices de Clasificación	7.2.1	9.2.4	Clasificación de la Información
Etiquetado y Manipulado de la Información	7.2.2	9.2.5	Marcado y Manejo de la Información
SEGURIDAD DE LOS RECURSOS HUMANOS	**8**	**9.3**	**SEGURIDAD ASOCIADA AL RECURSO HUMANO**
Antes del Empleo	**8.1**		

UNE-ISO/IEC 27002:2009		MAS	
Funciones y Responsabilidades	8.1.1	9.3.1	Responsabilidades y Perfiles de Puestos
Investigación de Antecedentes	8.1.2	9.3.2	Revisión de Antecedente y Referencias Personales
Términos y Condiciones de Contratación	8.1.3	9.3.3	Términos y Condiciones de Contrataciones
Durante el Empleo	**8.2**		
Responsabilidad de la Dirección	8.2.1		SECCIÓN 5: Responsabilidades de la Organización
Concienciación, Formación y Capacitación en Seguridad de la Información	8.2.2	9.3.4	Conocimiento Sobre la Documentación del SGSI
		9.3.5	Capacitación en Seguridad de la información
Proceso Disciplinario	8.2.3		SECCION 10: Incumplimiento a las Políticas y Lineamientos
Cese del Empleo o Cambio de Puesto de Trabajo	**8.3**		
Responsabilidad del Cese o Cambio	8.3.1	9.3.6	Cambio o Cese de Funciones
Devolución de Activos	8.3.2	9.3.7	Devolución de Activos
Retirada de los Derechos de Acceso	8.3.3	9.3.8	Revocación de Derechos de Acceso
SEGURIDAD FISICA Y AMBIENTAL	**9**	**9.4**	**SEGURIDAD FISICA Y AMBIENTAL**
Áreas Seguras	**9.1**		
Perímetro de Seguridad Física	9.1.1	9.4.1	Seguridad Física
Controles Físicos de Entrada	9.1.2	9.4.2	Control de Acceso Físico a la Información Confidencial o Reservada
Seguridad de Oficinas, Despachos e Instalaciones	9.1.3		
Protección contra Amenazas Externas y de Origen Ambiental	9.1.4	9.4.3	Protección Contra Amenazas Externas y del Ambiente
El Trabajo en Áreas Seguras	9.1.5	9.4.4	Trabajos en Áreas Seguras
Seguridad de los Equipos	**9.2**		
Emplazamiento y Protección de Equipos	9.2.1	9.4.5	Ubicación de Sistemas de Cómputo y Equipos de Producción
		9.4.7	Protección de Equipos Informáticos que Contengan Información
Instalaciones de Suministro	9.2.2	9.4.6	Servicios de Soporte
Seguridad del Cableado	9.2.3	9.4.8	Cables Eléctricos y de Telecomunicaciones
Mantenimiento de los Equipos	9.2.4	9.4.9	Mantenimiento Preventivo y Correctivo
Seguridad de los Equipos Fuera de las Instalaciones	9.2.5	9.4.10	Seguridad de los Equipos Fuera de las Instalaciones
Reutilización o Retirada Segura de Equipos	9.2.6	9.4.11	Disposición Final o Reutilización de Equipos
Retirada de Materiales Propiedad de la Empresa	9.2.7	9.4.12	Autorización para Salida de Equipos
GESTION DE COMUNICACIONES Y OPERACIONES	**10**	**9.5**	**GESTION DE COMUNICACIONES Y OPERACIONES**
Responsabilidades y Procedimientos de Operación	**10.1**		

UNE-ISO/IEC 27002:2009		MAS	
Documentación de los Procedimientos de Operación	10.1.1	9.5.1	Documentación de Sistemas y Procedimientos Operativos
Gestión de Cambios	10.1.2	9.5.2	Gestión de Cambios
Segregación de Tareas	10.1.3	9.5.3	Separación de Funciones
Separación de los Recursos de Desarrollo, Prueba y Operación	10.1.4	9.5.4	Separación de Ambientes de Desarrollo, Prueba y Producción
Planificación y Aceptación del Sistema	**10.3**		
Gestión de Capacidades	10.3.1	9.5.5	Gestión de la Capacidad
Aceptación del Sistema	10.3.2	9.5.6	Aceptación de Sistemas y Aplicaciones de Producción
Protección Contra Código Malicioso y Descargable	**10.4**		
Controles contra el Código Malicioso	10.4.1	9.5.7	Código Malicioso
Controles contra el Código Descargado en el Cliente	10.4.2	9.5.8	Configuración de Software y Controles de Seguridad de Equipos Cliente
Copias de Seguridad	**10.5**		
Copias de Seguridad de la Información	10.5.1	9.5.9	Respaldo de la Información en Medios Magnéticos
Gestión de la Seguridad de las Redes	**10.6**		
Controles de Red	10.6.1	9.5.10	Controles de Red de Datos
Seguridad de los Servicios de Red	10.6.2	9.5.11	Seguridad en los Servicios de Red de Datos
Manipulación de los Soportes	**10.7**		
Retirada de los Soportes	10.7.2	9.5.12	Eliminación de los Soportes
Procedimientos de Manipulación de la Información	10.7.3	9.5.13	Utilización de la Información
Seguridad de la Documentación del Sistema	10.7.4		
Intercambio de Información	**10.8**		
Políticas y Procedimientos de Intercambio de Información	10.8.1	9.5.14	Intercambio de Información y Software
Acuerdos de Intercambio	10.8.2		
Soportes Físicos en Tránsito	10.8.3	9.5.15	Soportes Físicos en Tránsito
Mensajería Electrónica	10.8.4	9.5.16	Mensajería Electrónica
Sistemas de Información Empresariales	10.8.5	9.5.17	Seguridad en la Interconexión de Sistemas de Información de Negocios
Servicios de Comercio Electrónico	**10.9**		
Comercio Electrónico	10.9.1	9.5.18	Comercio Electrónico
Transacciones en Línea	10.9.2	9.5.19	Pagos a Empleados y Terceros
Información Puesta a Disposición Pública	10.9.3	9.5.20	Información Disponible al Público
Supervisión	**10.10**		
Registro de Auditorias	10.10.1	9.5.21	Registros o Huellas de Auditoria
Registro de Administración y Operación	10.10.4		
Supervisión del Uso del Sistema	10.10.2		SECCION 4.2.3: Supervisión y Revisión del

UNE-ISO/IEC 27002:2009		MAS	
			SGSI
Protección de la Información de los Registros	10.10.3	9.5.22	Protección de los Registros o Huellas de Auditoría
Registros de Fallos	10.10.5	9.5.23	Registros de Fallas
Sincronización del Reloj	10.10.6	9.5.24	Sincronización del Reloj
CONTROL DE ACCESO	**11**	**9.6**	**CONTROL DE ACCESOS**
Requisitos de Negocio para el Control de Acceso	**11.1**		
Política de Control de Acceso	11.1.1	9.6.1	Política de Control de Acceso
Gestión de Acceso de Usuario	**11.2**		
Registro de Usuario	11.2.1	9.6.2	Registro de Usuarios
		9.6.5	Directorios de Usuarios
Gestión de Privilegios	11.2.2	9.6.3	Gestión de Privilegios
Gestión de Contraseñas de Usuario	11.2.3	9.6.4	Gestión de Contraseñas de Usuario
Revisión de los Derechos de Acceso de Usuario	11.2.4	9.6.6	Revisión de los Derechos de Acceso de Usuario
Responsabilidades de Usuario	**11.3**		
Uso de Contraseña	11.3.1	9.6.7	Uso y Estructura de las Contraseñas
Equipo de Usuario Desatendido	11.3.2	9.6.8	Computadores Desatendidos
Control de Acceso a la Red	**11.4**		
Política de Uso de los Servicios en Red	11.4.1	9.6.9	Uso de los Servicios de Red
Autenticación de Usuario para Conexiones Externas	11.4.2	9.6.10	Autenticación de Conexiones Externas
Diagnóstico Remoto y Protección de los Puertos de Configuración	11.4.4	9.6.11	Diagnostico Remoto y Protección de los Puertos de Configuración
Segregación de las Redes	11.4.5	9.6.12	Segregación de Redes de Datos
Control de la Conexión a la Red	11.4.6	9.6.13	Control de Conexiones a la Red
Control de Acceso al Sistema Operativo	**11.5**		
Procedimientos Seguros de Inicio de Sesión	11.5.1	9.6.14	Procedimientos para Inicio de Sesión
Identificación y Autenticación de Usuario	11.5.2	9.6.15	Identificación y Autenticación de Usuario
Sistema de Gestión de Contraseñas	11.5.3	9.6.7	Uso y Estructura de las Contraseñas
Uso de los Recursos del Sistema	11.5.4	9.6.16	Uso de los Recursos del Sistema
Control de Acceso a las Aplicaciones y a la Información	**11.6**		
Restricción del Acceso a la Información	11.6.1	9.6.20	Computadores Portátiles con Información Reservada o Confidencial
		9.6.17	Software Estándar en Estaciones de Trabajo
		9.6.18	Desinstalación de Herramientas
Ordenadores Portátiles y Teletrabajo	**11.7**		
Ordenadores Portátiles y Comunicaciones Móviles	11.7.1	9.6.19	Instalación o Desinstalación de Software

UNE-ISO/IEC 27002:2009		MAS	
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**12**	**9.7**	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION**
Requisitos de Seguridad de los Sistemas de Información	**12.1**		
Análisis y Especificación de los Requisitos de Seguridad	12.1.1	9.7.1	Análisis y Especificación de los Requisitos de Seguridad
Tratamiento Correcto de las Aplicaciones	**12.2**		
Validación de los Datos de Entrada	12.2.1	9.7.2	Validación de los Datos de Entrada
Control del Procesamiento Interno	12.2.2	9.7.3	Control del Procesamiento Interno
		9.7.6	Control de las Aplicaciones del Negocio en Producción
		9.7.7	Falla de las Aplicaciones del Negocio
		9.7.8	Retroalimentación de las Aplicaciones del Negocio al Usuario
Integridad de los Mensajes	12.2.3	9.7.4	Integridad de los Mensajes
Validación de los Datos de Salida	12.2.4	9.7.5	Validación de los Datos de Salida
Seguridad de los Archivos de Sistema	**12.4**		
Control del Software en Explotación	12.4.1	9.7.9	Prueba de las Aplicaciones del Negocio
		9.7.10	Instalación de las Aplicaciones del Negocio en Producción
Protección de los Datos de Prueba del Sistema	12.4.2	9.7.11	Protección de los Datos de Prueba del Sistema
Control de Acceso a Código Fuente de los Programas	12.4.3	9.7.12	Control de Acceso a Código Fuente de los Programas
Seguridad en los Procesos de Desarrollo y Soporte	**12.5**		
Procedimientos de Control para Cambios	12.5.1	9.7.13	Procedimiento de Control de Cambios
		9.7.14	Control de Cambios del Código Fuente
Revisión Técnica de las Aplicaciones tras efectuar Cambios en el Sistema Operativo	12.5.2	9.7.15	Revisión Técnica de las Aplicaciones tras Efectuar Cambios en el Sistema Operativo
Desarrollo de Software por Terceros	12.5.5	9.7.16	Desarrollo de Software por Terceros
Gestión de la Vulnerabilidad Técnica	**12.6**		
Control de las Vulnerabilidades Técnicas	12.6.1	9.7.17	Control de Vulnerabilidades de Software
GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	**13**	**9.8**	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**
Notificación de Eventos y Puntos Débiles de la Seguridad de la Información	**13.1**		
Notificación de los Eventos de Seguridad de la Información	13.1.1	9.8.1	Notificación de los Eventos de Seguridad de la Información
Gestión de Incidentes de Seguridad de	**13.2**		

UNE-ISO/IEC 27002:2009		MAS	
la Información y Mejoras			
Responsabilidades y Procedimientos	13.2.1	9.8.2	Responsabilidades y Procedimientos de Gestión de Incidentes de Seguridad
Aprendizaje de los Incidentes de Seguridad de la Información	13.2.2	9.8.3	Base de Conocimiento sobre Incidentes de Seguridad
GESTION DE LA CONTINUIDAD DEL NEGOCIO	**14**	**9.9**	**GESTION DE CONTINUIDAD DEL NEGOCIO**
Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	**14.1**		
Inclusión de la Seguridad de la Información en el Proceso de Gestión de la Continuidad del Negocio	14.1.1	9.9.1	Seguridad de la información en el Proceso de Continuidad del Negocio
Continuidad del Negocio y Evaluación de Riesgos	14.1.2	9.9.2	Continuidad del Negocio y Evaluación de Riesgos
Desarrollo e Implantación de Planes de Continuidad del Negocio que Incluyan la Seguridad de la Información	14.1.3	9.9.3	Desarrollo e Implantación de Planes de Continuidad del Negocio que Incluyan la Seguridad de la Información
Prueba, Mantenimiento y Reevaluación de los Planes de Continuidad del Negocio	14.1.5	9.9.4	Pruebas, Mantenimiento y Reevaluación de los Planes de Continuidad del Negocio
CUMPLIMIENTO	**15**	**9.10**	**CONFORMIDAD**
Cumplimiento con los Requisitos Legales	**15.1**		
Identificación de la Legislación Aplicable	15.1.1	9.10.1	Identificación de la Legislación Aplicable
Derechos de Propiedad Intelectual	15.1.2	9.10.2	Registro de Software de Desarrollo Interno y Derechos de Autor
Cumplimiento de las Políticas y Normas de Seguridad y Cumplimiento Técnico	**15.2**		
Cumplimiento de las Políticas y Normas de Seguridad	15.2.1	9.10.3	Cumplimiento de las Políticas y Normas de Seguridad SECCION 8.2 Acciones Correctivas SECCION 8.3 Acciones Preventivas
Consideraciones sobre la Auditoria de los Sistemas de Información	**15.3**		
Controles de Auditoría de los Sistemas de Información	15.3.1		SECCIÓN 6: Auditoría Interna al SGSI
Protección de las Herramientas de Auditoría de los Sistemas de Información	15.3.2	9.10.4	Protección de Herramientas de Auditoría

SECCIÓN 12: MODIFICACIONES

REGISTRO DE MODIFICACIONES

Nº	MODIFICACIONES
01	Se revisó la redacción y ortografía en todo el documento.
02	Sección 3. Términos y Definiciones Se eliminaron las siguientes definiciones: “Criptografía, Pasarela (Gateway).
03	Sección 4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ✓ En los numerales 4.2.1, 4.2.2, 4.2.3 y 4.2.4 se incorporó introducción en cada uno de los numerales. ✓ Se modificaron los siguientes numerales: 4.2.1 literales b) y h). 4.3.1 Se cambió el orden en el que estaban colocados.
04	Sección 5. RESPONSABILIDADES DE LA ORGANIZACIÓN ✓ Se modificaron los siguientes numerales: 5.1.1.1 literal f), 5.1.2.9. ✓ Se incorporaron las siguientes responsabilidades en el numeral 5.1.2 RESPONSABILIDADES DE LA ORGANIZACIÓN: 5.1.2.10 Especialista en Ciberseguridad de la DINAFI y 5.1.2.11 Técnico de Monitoreo de Ciberseguridad de la DINAFI.
05	Sección 6. AUDITORIA INTERNA AL SGSI: Se modificó el último párrafo de la Sección.
06	Sección 9. Lineamientos. Se modifican los siguientes apartados: 9.2.3, 9.3.8, 9.4.2, 9.4.5, 9.4.6, 9.5.15