Tabla de contenido

TABLA DE CONTROL DE CAMBIOS			
VERSIÓN	FECHA	SECCIONES MODIFICADAS	DESCRIPCIÓN GENERAL DE CAMBIOS
0(Cero)	27.11.2019	Elaboración inicial	Todas

ELABORADO POR	APROBADO POR
JEFE DE UNIDAD DE INFORMÁTICA	JEFE/A DE DIVISIÓN DE PLANIFICACIÓN Y PRESUPUESTO
GUSTAVO ASCENCIO C.	EUGENIO QUEZADA E.

1. OBJETIVOS

Obtener información de forma oportuna de las vulnerabilidades de los sistemas de información que permita evaluar las medidas necesarias y mitigar riesgos detectados.

2. ALCANCE

Se aplica a las instalaciones de procesamiento de información existentes en el MBN y que dan soporte a todos los procesos de provisión de bienes y servicios de la institución.

3. ROLES Y RESPONSABILIDADES

Rol	Responsabilidad
Encargado de Seguridad de la Información (ESI)	Controlar la aplicación de esta política.
Encargado de Ciberseguridad	Controlar la aplicación de esta política.

4. POLÍTICA

- Se debe mantener el inventario de activos de la información actualizado de acuerdo con el procedimiento **TIC-SI-P1 Actualización de Inventario de Activos**.
- Se debe estar suscrito a las publicaciones que los proveedores de software publican en cuanto a vulnerabilidades técnicas descubiertas. Para ello, el área de informática debe tener el listado de software utilizado en sus operaciones diarias y, adicionalmente, tener el listado de software utilizado por el personal del MBN.
- Se deben definir roles y responsabilidades en la gestión de vulnerabilidades técnicas para las siguientes actividades:
  - Monitoreo periódico de las vulnerabilidades
  - Evaluación de los riesgos de las vulnerabilidades
  - Mitigación de las vulnerabilidades detectadas
- Se debe definir la herramienta informática que será utilizada para identificar las vulnerabilidades de los activos de información.
- Se debe definir un procedimiento para abordar el caso en que se detecte una vulnerabilidad, el cuál debe quedar documentado:
  - Definir un tiempo de reacción frente a la notificación de una vulnerabilidad.
  - Identificar riesgos frente a la vulnerabilidad.
  - Establecer la urgencia para abordar la vulnerabilidad.
  - Evaluar y probar los parches en ambiente de QA que corrigen la vulnerabilidad.
- Si no es posible realizar pruebas a los parches por la falta de recursos, se puede considerar un retraso en la instalación debiendo evaluar los riesgos asociados.

- El tratamiento de incidentes, y los cambios asociados en los sistemas, deben realizarse de acuerdo a los procedimientos **TIC-SI-P2 Respuesta ante incidentes de Seguridad de la Información** y lo dispuesto en el **Manual de Desarrollo Seguro.**
- La detección de vulnerabilidades técnicas debe alinearse con los lineamientos presidenciales sobre ciberseguridad.

5. DEFINICIONES Y ABREVIATURAS

MBN: Ministerio de Bienes Nacionales.
SGSI: Sistema de Gestión de Seguridad de la Información.
PARCHE: Cambio que se realiza a un sistema de información para corregir un error.
QA: Ambiente de prueba previo al paso a Producción

6. DIFUSIÓN

La difusión de esta política se realizará mediante el envío de correos electrónicos a todos/as los/las funcionarios/as y personal externo del MBN, relacionados al ámbito de esta política, además de su publicación en la Intranet institucional.

7. REVISIÓN

Toda política debe ser revisada y evaluada al menos una vez al año o cuando se produzcan cambios en las normativas y leyes que regulan el accionar del ministerio o cuando el Jefe de Servicio así lo disponga.

Para su revisión se podrá tomar en cuenta la evaluación de los riesgos de seguridad de información, el resultado de auditorías internas o externas, cambios en las tecnologías, cambios en la organización del ministerio, así como la ocurrencia de incidentes de Seguridad, que afecte al SGSI.

8. PROCESOS DISCIPLINARIOS

El incumplimiento o violación a las políticas y procedimientos de seguridad, debidamente acreditado, conlleva a un proceso disciplinario formal avalado por la normativa vigente y Estatuto Administrativo según corresponda, a los funcionarios, personal a honorarios y contratos de prestaciones de servicios, o al termino anticipado del contrato por incumplimiento de las obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren en el alcance de esta política, sin perjuicio de las responsabilidades civiles y penales que deriven de tales infracciones.

DOCUMENTOS DE REFERENCIA.	
1.	TIC-SI-POL-1 Política general de seguridad de la información.
2.	ISO 27001:2013 A.12.06.01 Gestión de las vulnerabilidades técnicas.
3.	Manual de Desarrollo Seguro del MBN.
4.	TIC-SI-P2 Procedimiento de respuesta ante incidentes de Seguridad de la Información.
5.	TIC-SI-P1 Procedimiento de Actualización de Inventario de Activos