POLÍTICA DE MONITOREO CONTINUO Y GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre y Apellido / Cargo	Firma
Elaborado por:	Ing. Geovanny Meza, Mg. **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: JORGE GEOVANNY MEZA MORALES
Revisado y aprobado por:	Ing. Patricio Padrón **Director de Tecnologías de la Información y Comunicación**	Firmado electrónicamente por: NARDO PATRICIO PADRON CORREA

ÍNDICE

1. Notas del Cambio

Versión	Fecha	Detalle de la modificación
1	09/12/2021	Creación de la política

2. Antecedentes

El Esquema Gubernamental de Seguridad de la Información (EGSI), establece una serie de hitos que contemplan la elaboración, implementación y difusión, de políticas, procedimientos, reglamentos, normas y demás instrumentos técnicos, que garanticen el manejo seguro de la información de las instituciones públicas.

Ningún sistema, aplicación, software o equipo de cómputo es infalible, por lo que se pueden presentar vulnerabilidades que podrían ser aprovechadas para acceder a los mismos, poniendo en riesgo la información institucional. Es por ello que se vuelve imprescindible contar con un conjunto de políticas de monitoreo y gestión de vulnerabilidades técnicas, que permitan garantizar en la medida de lo posible, la seguridad de la información.

3. Alcance

El registro aquí descrito es de uso exclusivo de la Dirección de Tecnologías de la Información y Comunicación; por lo que al alcance del mismo es a dicha instancia del Secap.

4. Propósito

Definir las políticas a partir de las cuales se realizará el monitoreo continuo y la gestión de vulnerabilidades técnicas.

5. Definiciones

- **Análisis de log:** Estudio de los logs para identificar eventos de interés o suprimir entradas de eventos insignificantes.
- **Aplicaciones de software:** Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.

- **Contraseña:** Código secreto compuesto por una cadena de caracteres que pueden ser especiales y alfanuméricos, que se introduce en un sistema, equipo informático o red para iniciarlo y acceder para operarlo.
- **Credenciales de acceso:** Son el nombre de usuario y contraseña gestionados que dan acceso a un sistema o equipo.
- **Evento:** Una alerta o notificación creada por algún componente de la plataforma tecnológica de la información o herramienta de monitoreo.
- **Incidente:** Es un evento o serie de eventos de seguridad de la información no deseado o no planeado, que afecte la prestación del servicio o reduzca la calidad de la prestación del servicio o que tenga una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Internet:** Red mundial de computadores conectadas entre sí que ofrecen acceso y comparten información a través de un lenguaje común.
- **Intranet:** Red informática interna basada en los estándares de internet.
- **Log:** Es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema. Se utiliza en muchos casos distintos, para guardar información sobre la actividad de sistemas variados.
- **Registro de eventos:** Es un documento que registra datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre en un dispositivo en particular, aplicación o sistema.
- **Seguridad del sistema:** Conjunto de medidas preventivas y correctivas que permiten resguardar y proteger la información y los sistemas de software que la procesan y almacenan.
- **Servicios:** Conjunto de aplicativos o programas informáticos y de comunicación de datos que apoyan la labor del Secap.
- **Servidor/funcionario:** Persona que presta servicios a la Administración o a nombre y por cuenta de esta, como parte de su organización, en virtud de un acto válido y eficaz de investidura, con entera independencia del carácter imperativo, representativo, remunerado, permanente o público de la actividad respectiva.

- **Sistema de software:** Programas informáticos diseñados con el propósito de facilitar a los usuarios la realización de determinadas tareas.
- **Usuario:** Nombre o identificador compuesto por una cadena de caracteres alfanuméricos, que emplea una persona para identificarse en un sistema, equipo o red, previo a ingresar la contraseña.
- **VPN:** Virtual Private Network o red privada virtual, es una conexión en línea caracterizada por ser segura y estar cifrada (codificada) que permite establecer comunicación desde un equipo remoto a una red empresarial o institucional.

6. Políticas

- Para un adecuado monitoreo continuo y gestión de vulnerabilidades técnicas, es obligatorio considerar las Políticas de Registro y Administración de Operación; y, las Políticas de Registro de Eventos.
- El monitoreo continuo de los diferentes sistemas, aplicaciones, sistemas, red de datos, internet y comunicaciones, es responsabilidad de los administradores que han sido designados formalmente.
- El Gestor de Administración de Servicios, Componentes de TI y Soporte Técnico a Usuarios, se encargará de elaborar un formato para el monitoreo continuo y reporte de vulnerabilidades, de los diferentes sistemas, aplicaciones, sistemas, red de datos, internet y comunicaciones.
- Los administradores de los diferentes sistemas, aplicaciones, sistemas, red de datos, internet y comunicaciones, deben reportar al Director de Tecnologías de la Información y Comunicación, de forma mensual y en los 10 primeros días de cada mes, un informe de monitoreo.
- El monitoreo continuo y gestión de vulnerabilidades técnicas, puede hacerse también de forma remota, para lo cual, el gestor a cargo solicitará al Director de Tecnologías de la Información y Comunicación, la autorización y accesos a la red privada virtual, en caso de requerirlo.
- En caso de identificarse vulnerabilidades, el gestor a cargo deberá remitir al Director de Tecnologías de la Información y Comunicación, un plan de trabajo encaminado a resolver o minimizar la situación, en el menor tiempo posible.

- El Director de Tecnologías de la Información y Comunicación es responsable de gestionar, ante las autoridades competentes, los recursos necesarios para el monitoreo continuo y la gestión de vulnerabilidades.
- En caso de que no se dispongan de los recursos para solventar la gestión de vulnerabilidades, el Director de Tecnologías de la Información y Comunicación deberá remitir un informe a la máxima autoridad institucional, en el cual dé a conocer el particular y las posibles soluciones.

7. Anexos

Ninguno.