DOCUMENTO DE GESTIÓN

Proyecto: Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y Empresas a Nivel Nacional - SGSI

Versión: 1.0

Registro de Cambios				
Versión	**Páginas**	**Fecha**	**Descripción**	**Autor**
1.0	5	08-03-2022	Versión inicial	Andrés Cómina Jara

Control documental		
	Preparado y revisado por	**Aprobado por**
Nombre **Rol**	Andrés Cómina Jara Responsable del SGSI de la PNGD	Manuel Humberto Valdera García Subsecretario (e) de la Subsecretaría de Tecnología y Seguridad Digital
Fecha	08-03-2022	10-03-2022

ÍNDICE

1. INTRODUCCIÓN

El objetivo de crear la política de seguridad de la información en relación con el acceso físico, para la Plataforma Nacional de Gobierno Digital (PNGD), en la Secretaría de Gobierno y Transformación Digital (SGTD), dentro de la Presidencia del Consejo de Ministros (PCM), es establecer los compromisos y el marco general (legal y regulatorio) para gestionar los riesgos asociados al acceso a cada una de las sedes que sean necesarios para la prestación de los servicios ofrecidos a fin de minimizar riesgos de seguridad de la información y prevenir las amenazas a los activos de información ubicados en dichas sedes.

2. DEFINICIONES

Activos de información: Todo aquello que es o contiene información que es de valor para la PNGD. Por ejemplo: documentos digitales o físicos, servicios, aplicaciones, equipos, entre otros activos que la organización valora y protege de cualquier vulnerabilidad que amenaza con la divulgación, indisponibilidad y pérdida de integridad de la información.

Amenazas: Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

Amenazas físicas: Relativo al acceso físico a los recursos, pueden causar robos, daños físicos a los activos de información.

Riesgos: Las amenazas de ataques y las vulnerabilidades de la tecnología.

Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de los activos de información.

3. ALCANCE

Las sedes físicas en las que se encuentran los activos de información utilizados en la prestación de los servicios ofrecidos por la PNGD.

4. OBJETIVOS

a) Definir y formalizar una política alineada a los marcos legales y regulatorios (de la PCM, SGTD y PNGD), que ayudarán a la empresa a mitigar los riesgos de seguridad de la información en la relación con el acceso físico en las sedes de la PNGD, en las cuales se brindan los servicios ofrecidos por la PNGD.

b) Establecer compromisos con la finalidad de monitorear, registrar, controlar un adecuado acceso físico a las sedes de la PNGD, a fin de minimizar riesgos de seguridad de la información y prevenir las amenazas sobre los activos de información involucrados en la prestación de los servicios ofrecidos por la PNGD.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – ACCESO FÍSICO

La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital (SGTD), gestiona el acceso físico como parte de la gestión eficiente de la seguridad de la información, la mitigación de los riesgos de seguridad de la información, a fin prevenir la pérdida y/o daño de los activos de información ubicados en las sedes de la PCM y/o desde donde se ofrecen los servicios de la PNGD.

Para la ejecución adecuada en materia de seguridad de la información en lo que refiere al acceso físico, la SGTD asume los siguientes compromisos:

1. Difundir la política de seguridad de la información en lo que refiere al acceso físico.
2. Establecer las zonas de acceso permitido en las sedes de la SGTD para el personal de la PNGD.
3. Establecer las zonas de acceso permitido en la sede de la PNGD.
4. Establecer, comunicar y controlar el personal de la PNGD que tendrá acceso a las zonas permitidas de las sedes de la SGTD.
5. Llevar a cabo un registro del acceso físico de ingreso y salida a cada una de las sedes en las cuales la PNGD tenga instalados activos de información.
6. Cruzar información de acceso físico entre los registros de los administradores de las sedes en las cuales la PNGD tenga instalados activos de información y los registros propios de la PNGD.
7. Monitorear el cumplimiento del acceso físico autorizado, sólo a áreas permitidas durante las actividades a ejecutar por los proveedores en cualquiera de las sedes donde se realiza el servicio ofrecido por la PNGD.
8. Asignar personal responsable para generar autorizaciones de acceso al personal interno o externo en cada una de las sedes.
9. Determinar los equipos y/o activos con las que puede tener contacto físico cada persona en cada una de las áreas de trabajo asignadas.

10. Exigir a los proveedores de la PNGD que se identifiquen, se registren y comuniquen cada objeto y/o activo de información que lleven consigo durante la visita a alguna sede involucrada en el servicio.

11. Documentar todas las excepciones que se hayan aprobado al cumplimiento de la presente política.