CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de acceso remoto

Versión 1.0

APROBACIONES

Elaborado por:	Revisado por:	Aprobado por:
<Nombre>	<Nombre>	<Nombre>
<Cargo>	<Cargo>	<Cargo>
<Firma>	<Firma>	<Firma>

HISTORIAL DE REVISIONES

Versión	Fecha	Revisión
1.0	Diciembre 2021	Versión Inicial

Contenido

1. Introducción

1.1 Autoridad

El Centro Nacional de Seguridad Digital fue creado el 9 de enero del 2020, mediante Decreto de Urgencia N° 007-2020, es el encargado de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. También es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital.

1.2 Propósito

El propósito de esta política es definir las actividades asociadas con la provisión de seguridad de acceso para empleados y no empleados autorizados que trabajan de forma remota para proteger la organización, sistemas de información, redes, datos, bases de datos y otros activos de información de eventos de ciberseguridad y seguridad de la información que puedan ocurrir mientras están en uso por trabajadores remotos.

1.3 Alcance

Esta política se aplica a todos los empleados y afiliados de la organización.

2. Política

2.1 Se debe definir controles de confidencialidad, integridad y disponibilidad para los usuarios de acceso remoto.
2.2 Se debe definir una lista de servicios, redes y sistemas de información que puedan ser utilizados remotamente por el personal que realiza el acceso.
2.3 Se debe contar con un inventario de accesos remotos otorgados, identificando a la persona que cuenta con el acceso, el motivo por el cual se le otorgó y el plazo por el cual está autorizado.
2.4 Los equipos utilizados para el acceso remoto deben contar con protección ante software malicioso.
2.5 Los equipos utilizados para el acceso remoto deben estar cifrados.
2.6 Se debe definir un procedimiento de revisión periódica de las condiciones de uso del acceso remoto y de los usuarios que hacen uso de éste.
2.7 Se debe monitorear y analizar el tráfico de datos de acceso remoto para identificar posibles anomalías de seguridad.
2.8 Se debe planificar e impartir capacitaciones de concientización para empleados y miembros del equipo en temas de ciberseguridad y seguridad de la información.
2.9 Se debe redactar un documento donde se contemplen todas las acciones realizadas en acceso remoto (duración, dispositivos facilitados, entre otros), el cual debe ser firmado por cada usuario.
2.10 Se debe valorar diferentes escenarios y configuraciones antes de habilitar el acceso remoto, contemplando todos los riesgos de seguridad digital.
2.11 Se debe gestionar las credenciales de acceso de los usuarios forzando el uso de contraseñas robustas y su cambio periódico, además de incluir el doble factor de autenticación.
2.12 Se debe configurar los dispositivos utilizados por el usuario para el trabajo en acceso remoto (sistema operativo, antivirus, control de actualizaciones, entre otros) tanto si son corporativos o aportados por el usuario.
2.13 Se debe elaborar las políticas que detallen a los usuarios dónde deben guardar la información con la que trabajan en remoto.
2.14 Se debe planificar las copias de seguridad de todos los soportes y comprobar que puedan ser restauradas.
2.15 Se debe usar conexiones seguras a través de una red privada virtual o VPN.
2.16 Se debe evitar conexión a redes wi-fi públicas.
2.17 Se debe llevar a cabo auditorías periódicas para asegurar el cumplimiento de la política.

3. Cumplimiento de políticas

3.1.1 Medición de cumplimiento

Se verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, recorridos periódicos, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas y comentarios al propietario de la póliza.

3.1.2 Excepciones

Cualquier excepción a la política debe ser aprobada con anticipación.

3.1.3 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, hasta e incluyendo la terminación del empleo.