CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de equipos de comunicaciones

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 establecer los requisitos mínimos para las configuraciones de seguridad de "equipos de comunicaciones".

1.3 Alcance

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

2. Política

2.1 Las características de seguridad necesarias para minimizar los riesgos para los equipos de comunicación deben configurarse en el equipo antes de su puesta en servicio.

2.2 Debe haber dos roles posibles para el personal que administra el equipo de comunicación: supervisor y administrador.

2.3 El rol de supervisor debe tener privilegios de solo lectura.

2.4 El rol de administrador debe poder cambiar los parámetros de configuración.

2.5 Se debe registrar todos los comandos emitidos por los usuarios en un log, así como cualquier otro evento de seguridad que pueda representar una amenaza para el equipo.

2.6 Los usuarios locales no están permitidos en los equipos de comunicación.

2.7 Todos deben autenticarse a través del repositorio central de usuarios utilizando un protocolo que reduce el riesgo de robo de identidad.

2.8 Toda la información transmitida desde el dispositivo debe estar cifrada por un algoritmo de cifrado fuerte para minimizar los riesgos de espiar las comunicaciones y los ataques man-in-the-middle.

2.9 Los eventos registrados por el equipo de comunicación deben mantenerse en medios de almacenamiento que estén sujetos a un proceso de copia de seguridad regular, es conveniente que estos eventos o logs se envíen a un centralizador de logs.

2.10 El proceso de mantenimiento de las copias de seguridad debe garantizar que la información no se modifique.

2.11 Si, por cualquier motivo, es necesario hacer uso de los más altos privilegios administrativos dentro del dispositivo, entonces el personal debe presentar una solicitud a la división de seguridad interna para la contraseña adjuntando la justificación de su uso y completando los formularios requeridos.

2.12 La contraseña debe ser restablecida por el administrador más alto para mantener la seguridad.

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.