CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de seguridad de la red

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 mantener la "seguridad de la red".

1.3 Alcance

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

2. Política

2.1 Se deben administrar y controlar las redes para proteger la información en los sistemas y aplicaciones.

2.2 Los usuarios privilegiados autorizados deben utilizar dispositivos dedicados que estén técnicamente segregados y asegurados al mismo nivel que las redes y los sistemas que se mantienen.

2.3 Los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios se proporcionen internamente o se subcontraten.

2.4 Todos los dispositivos de red, excepto los cortafuegos, deben ser accesibles desde dentro de la red privada.

2.5 Todas las conexiones de red deben pasar a través de un cortafuegos.

2.6 Se debe llevar a cabo una evaluación de riesgos antes de que se permitan enlaces y, cuando corresponda, se debe implementar medidas de seguridad adicionales.

2.7 La conectividad entrante a la red se debe permitir desde una VPN.

2.8 La conectividad entrante desde Internet se debe permitir a dispositivos designados en la DMZ usando Servicios TCP / IP.

2.9 Los cambios en el firewall deben pasar por solicitud y autorización.

2.10 Cada enrutador debe cumplir con la configuración estándar.

2.11 Cada enrutador y conmutador debe utilizar el proceso de autenticación y administración estándar.

2.12 Todas las contraseñas de enrutador / conmutador deben estar cifradas.

2.13 Los protocolos de enrutamiento dinámico deben utilizar la autenticación en las actualizaciones de enrutamiento.

2.14 El hash de contraseña para la cadena de autenticación debe estar habilitado cuando sea compatible.

2.15 El administrador de red debe verificar el cumplimiento de la política.

2.16 Los dispositivos inalámbricos deben cumplir las condiciones de esta política y ser aprobados para la conectividad a la red.

2.17 Los dispositivos deben ser instalados, respaldados y mantenidos por un equipo de soporte aprobado.

2.18 Los dispositivos deben usar protocolos de cifrado.

2.19 Se debe deshabilitar cualquier dispositivo que presente un riesgo para la red.

2.20 Se debe supervisar el tráfico entrante y saliente, y los flujos de datos de todos los puntos finales dentro de la red.

2.21 Se debe revisar la red continuamente de acuerdo con las mejores prácticas y utilización del proveedor.

2.22 Se debe realizar un control de cambios formal e incluir la actualización de la documentación y los diagramas de red que se almacenan de forma segura.

2.23 Se debe utilizar VLAN para proporcionar segmentación de la red cuando no se pueden aplicar políticas de seguridad corporativas.

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.