CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de control de acceso

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 5

1.1 AUTORIDAD 5
1.2 PROPÓSITO 5
1.3 ALCANCE 5

2. POLÍTICA 6

3. CUMPLIMIENTO DE POLÍTICAS 7

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 quién, cómo y cuándo puede acceder a los activos de información de la organización y registrar convenientemente dichos accesos.

1.3 Alcance

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

2. Política

2.1 Los sistemas deben contar con controles de acceso y medidas de seguridad adecuadas para la protección de su confidencialidad, integridad y disponibilidad.

2.2 Los usuarios deben tener acceso a las redes y servicios de red para los que hayan sido específicamente autorizados a utilizar. El acceso se registra y supervisa.

2.3 Se debe tener un registro formal de todas las personas registradas para utilizar el servicio con los detalles del autorizador.

2.4 Las cuentas de la red se deben cancelar por inactividad o como resultado de una actualización.

2.5 El área de recursos humanos de la organización deberá a intervalos definidos comunicar al área de tecnologías de información del personal que ha cesado en sus funciones, para de esta forma poder cancelar las cuentas de acceso.

2.6 Se debe asignar una ID de red única a los usuarios, que los vincula a ellos y sus acciones.

2.7 El acceso privilegiado debe seguir el principio de acceso mínimo del usuario, proporcionarse en función de las necesidades del trabajo con tan pocos privilegios como se requieran para su función laboral.

2.8 El personal no debe iniciar sesión en sus dispositivos como administrador.

2.9 Los derechos de acceso del usuario se deben revisar a medida que se notifican los cambios de función del usuario.

2.10 Las ID de usuario redundantes se deben eliminar de acuerdo con la Política de eliminación de cuentas de red.

2.11 Las ID de usuario que han estado inactivas durante 60 días se deben deshabilitar.

2.12 Se debe informar a los nuevos usuarios sobre la importancia de las contraseñas y se les instruye sobre la manera en que deben usarse y protegerse en la formación básica para nuevos empleados.

2.13 El acceso a la información debe ser controlada mediante la autorización del administrador y el Control de acceso basado en roles asignado a las cuentas de la aplicación.

2.14 Cada sistema debe tener una administración de contraseñas utilizando fuerza, longitud y complejidad.

2.15 Se debe restringir el uso de programas de utilidades privilegiadas y administrado por personal técnico con cuentas de usuario estándar que no tienen los derechos para instalar software.

2.16 Se debe restringir el acceso de terceros al código fuente del programa.

2.17 Se debe utilizar controles adicionales, cuando el acceso sea exterior como certificados de dos factores o respaldados por hardware.

2.18 Se debe desactivar automáticamente la cuenta, por intentos no autorizados.

2.19 Los propietarios de activos deben revisar los derechos de acceso de los usuarios individuales a las redes y sistemas que respaldan el servicio esencial a intervalos regulares.

2.20 Los derechos de acceso de todos los empleados y usuarios externos a la información y las instalaciones de procesamiento de información se deben eliminar al terminar su empleo, contrato o acuerdo, o se debe ajustar al cambiar.

2.21 Los usuarios deben seguir las prácticas de la organización en el uso de la información de autenticación secreta.

2.22 Se debe restringir el uso de programas de utilidad que puedan ser capaces de invalidar sistemas y aplicaciones.

2.23 Para el acceso a servidores se debe implementar de manera obligatoria como mínimo el doble factor de autenticación, se recomienda implementar el mismo mecanismo en las estaciones de trabajo.

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.