POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN - NEURODESK CORP

Versión: 4.2 | Última actualización: Noviembre 2025

1. CONTROL DE ACCESO Y CREDENCIALES

1.1. Contraseñas: Todos los empleados deben utilizar contraseñas de al menos 12 caracteres, incluyendo mayúsculas, números y símbolos.

1.2. Rotación: Las credenciales deben actualizarse cada 90 días. Si olvida su contraseña, debe utilizar el sistema automatizado de NeuroDesk (Runbook: Reset-ADPassword) para obtener una temporal.

1.3. Bloqueo de Cuenta: Tras 3 intentos fallidos, la cuenta se bloqueará automáticamente por 30 minutos salvo intervención de un administrador.

2. USO DE REDES Y VPN

2.1. Conexión Remota: El acceso a recursos internos (Intranet, SAP, Servidores de Archivos) fuera de la oficina requiere obligatoriamente el uso de la VPN Corporativa.

2.2. Inestabilidad: Si experimenta latencia superior a 200ms o desconexiones frecuentes, está autorizado a solicitar un reinicio del gateway a través del asistente virtual (Runbook: Restart-VPN-Gateway).

2.3. Redes Públicas: Está prohibido conectar equipos corporativos a redes Wi-Fi públicas (aeropuertos, cafeterías) sin la VPN activa.

3. GESTIÓN DE INCIDENTES Y LOGS

3.1. Reporte: Cualquier anomalía en el rendimiento de las aplicaciones debe ser reportada inmediatamente.

3.2. Evidencias: Para el análisis forense, los logs de error y capturas de pantalla deben subirse únicamente a través de enlaces seguros generados por el sistema (NeuroDesk-Generate-Upload-Link). Está prohibido enviar logs por correo electrónico o Teams debido a la posible exposición de datos sensibles.

4. MANTENIMIENTO DE EQUIPOS

4.1. Rendimiento: Si su equipo experimenta lentitud extrema o bloqueo de aplicaciones, utilice la herramienta de optimización automática (Self-Heal) antes de solicitar un cambio de hardware.

4.2. Actualizaciones: Los parches de seguridad críticos se instalan automáticamente los viernes a las 23:00.