Políticas Públicas

- POLÍTICA DE USO DE DISPOSITIVOS FINALES

POLÍTICA DE USO DE DISPOSITIVOS FINALES

Código: POL-SI-005

Versión: 1.0

Fecha de aprobación: XX/XX/2026

Propietario: Dirección General de Informática (DGI)

Clasificación: Uso Interno

1. Objetivo

Establecer los lineamientos para el uso seguro de los dispositivos finales utilizados para acceder a los recursos tecnológicos de la Universidad Católica "Nuestra Señora de la Asunción", reduciendo los riesgos asociados a pérdida de información, accesos no autorizados, malware, robo de credenciales y otros incidentes de seguridad.

2. Alcance

Esta política aplica a:

Funcionarios administrativos.
Docentes.
Investigadores.
Autoridades.
Contratistas.
Becarios.
Pasantes.
Personal temporal.
Todo usuario autorizado de los sistemas institucionales.

Comprende los siguientes dispositivos:

Computadoras de escritorio.
Computadoras portátiles.
Tablets.
Smartphones.
Equipos virtuales.

Equipos institucionales.
Equipos personales autorizados (BYOD).
3. Definiciones
Dispositivo final (Endpoint)

Equipo utilizado por un usuario para acceder a recursos tecnológicos institucionales.

Equipo institucional

Dispositivo adquirido y administrado por la Universidad.

Equipo personal (BYOD)

Equipo propiedad del usuario autorizado para acceder a servicios institucionales.

Información institucional

Toda información producida, almacenada o procesada por la Universidad.

4. Responsabilidades
Dirección General de Informática

Será responsable de:

administrar las plataformas de gestión de dispositivos;
definir configuraciones de seguridad;
instalar software institucional;
aplicar actualizaciones;
responder a incidentes;
controlar el cumplimiento de esta política.
Responsables de cada unidad

Deberán:

velar por el correcto uso de los equipos asignados;
informar altas, bajas y cambios de usuarios;
comunicar incidentes.
Usuarios

Todo usuario deberá:

utilizar los equipos exclusivamente para actividades autorizadas;
proteger las credenciales de acceso;
reportar incidentes inmediatamente;
cumplir esta política.
5. Requisitos Generales

Todo dispositivo que acceda a recursos institucionales deberá cumplir como mínimo con los siguientes requisitos.

5.1 Sistema operativo

Debe encontrarse:

soportado por el fabricante;
actualizado;
con parches de seguridad instalados.

No se permitirá el uso de sistemas operativos fuera de soporte.

5.2 Antivirus

Los dispositivos deberán contar con:

solución antimalware aprobada por la DGI;
protección en tiempo real;
actualizaciones automáticas.
5.3 Firewall

El firewall del sistema operativo deberá permanecer habilitado.

No podrá ser deshabilitado por el usuario.

5.4 Actualizaciones

Las actualizaciones de seguridad deberán instalarse tan pronto como sea posible.

Los usuarios no deberán impedir las actualizaciones automáticas.

5.5 Software autorizado

Únicamente podrá instalarse software:

licenciado;
autorizado por la DGI;
necesario para las funciones laborales.

Se prohíbe instalar:

software pirata;
aplicaciones de origen desconocido;
herramientas de hacking no autorizadas;
software P2P;
criptominería;

software que comprometa la seguridad institucional.
6. Gestión de credenciales

Los usuarios deberán:

utilizar únicamente sus propias credenciales;
mantener confidenciales las contraseñas;
habilitar MFA cuando esté disponible;
bloquear el equipo al ausentarse.

Está prohibido:

compartir contraseñas;
almacenar contraseñas en papel visible;
guardar credenciales en archivos de texto.
7. Bloqueo automático

Los equipos deberán configurarse para:

bloquearse automáticamente luego de un período de inactividad;
requerir autenticación para reanudar la sesión.
8. Cifrado

Los dispositivos portátiles deberán utilizar cifrado de disco completo cuando sea técnicamente posible.

Ejemplos:

BitLocker
FileVault
LUKS
9. Almacenamiento de información

La información institucional deberá almacenarse preferentemente en:

servidores institucionales;
servicios en la nube autorizados;
repositorios administrados por la Universidad.

No deberá almacenarse información sensible de manera permanente en:

discos USB;
discos externos;
almacenamiento personal no autorizado.
10. Uso de dispositivos USB

Se permitirá únicamente cuando exista una necesidad institucional.

La DGI podrá restringir:

escritura;
lectura;
ejecución automática.

Todo dispositivo USB deberá ser analizado por el antivirus antes de utilizarse.

11. Uso de dispositivos personales (BYOD)

Los dispositivos personales podrán acceder a recursos institucionales únicamente cuando:

cumplan los requisitos mínimos de seguridad;
tengan antivirus actualizado;
utilicen autenticación fuerte;
acepten las políticas institucionales.

La Universidad podrá limitar el acceso de equipos que no cumplan estas condiciones.

12. Uso de redes

Los dispositivos deberán conectarse preferentemente mediante:

red institucional;
VPN institucional cuando corresponda.

Se recomienda evitar redes Wi-Fi públicas para acceder a información sensible.

13. Correo electrónico

Los usuarios deberán:

verificar remitentes;
evitar abrir archivos sospechosos;
reportar mensajes fraudulentos;
no reenviar cadenas de correos.
14. Navegación web

Está prohibido utilizar los dispositivos institucionales para:

descargar software ilegal;
acceder a sitios maliciosos;
ejecutar aplicaciones no autorizadas;
actividades que vulneren la legislación vigente.
15. Pérdida o robo

Ante pérdida o robo del dispositivo el usuario deberá comunicar inmediatamente a la DGI.

La Universidad podrá:

bloquear el acceso;
revocar certificados;
invalidar sesiones;
ejecutar borrado remoto cuando corresponda.
16. Monitoreo

La Universidad podrá realizar monitoreo de:

cumplimiento de configuraciones;
estado del antivirus;
versiones del sistema operativo;
eventos de seguridad;
inventario de hardware y software.

Este monitoreo tendrá fines exclusivamente institucionales y de seguridad.

17. Incumplimientos

El incumplimiento podrá dar lugar a:

suspensión del acceso a sistemas;
retiro del dispositivo institucional;
acciones disciplinarias;
acciones legales cuando corresponda.
18. Excepciones

Toda excepción deberá:

documentarse;
justificar el riesgo;
contar con aprobación de la Dirección General de Informática y de la autoridad competente;
establecer un plazo de vigencia.
19. Referencias

Esta política se fundamenta en:

ISO/IEC 27001:2022
ISO/IEC 27002:2022
NIST Cybersecurity Framework 2.0
CIS Controls Version 8
Legislación paraguaya aplicable en materia de protección de datos, delitos informáticos y firma electrónica.
Reglamento Interno de la Universidad Católica "Nuestra Señora de la Asunción".
Anexo A – Requisitos mínimos de seguridad

Todo dispositivo que acceda a recursos institucionales deberá cumplir, como mínimo, con los siguientes controles:

Control	Requisito
Sistema operativo soportado	Obligatorio
Actualizaciones automáticas	Obligatorio
Antivirus activo	Obligatorio
Firewall habilitado	Obligatorio
Bloqueo	