

POLITICA TRAE TU PROPIO DISPOSITIVO

Versión: 1

Código de documento: PO-GMG-2025-0006

Elaborado por: José Luis Robelo

Technology Core, S.A.

POLITICA TRAE TU PROPIO DISPOSITIVO

Código:	<i>PO-GMG-2025-0005</i>
Versión:	1
Fecha de la versión:	31/07/25
Creado por:	Gerencia de Operaciones
Visto Bueno:	Quality Assurance
Aprobado por:	Gerencia General
Nivel de confidencialidad:	2

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
31/07/25	1	José Luis Robelo	Creación del documento / Versión inicial

Firmas

FIRMANTE		FIRMA
Elaborado por	Jose Luis Robelo Cybersecurity Specialist Technology Core, S.A.	
Revisado por	Leonel Ordóñez Quality Assurance Technology Core, S.A.	
Aprobado por	Jason Galvez Chief Executive Officer Technology Core, S.A.	

CONTENIDO

FIRMAS	2
1. OBJETIVO, ALCANCE Y USUARIOS.....	4
2. ALCANCE DE LA POLÍTICA	4
3. USUARIOS A LOS QUE APLICA ESTA POLÍTICA	4
4. DOCUMENTOS DE REFERENCIA.....	4
5. POLÍTICAS PARA EL USO DE DISPOSITIVOS BYOD	4
5.1 POLÍTICA DE TECHCORE PARA BYOD.....	4
5.2 QUIEN TIENE PERMITIDO UTILIZAR BOYD.....	4
5.3 USO ACEPTABLE DE BYOD	4
5.4 VIOLACIONES DE SEGURIDAD	5

1. Objetivo, alcance y usuarios

El objetivo de esta política es definir cómo Techcore tendrá el control sobre su información, cuando la información perteneciente a Techcore es accedida y procesada por medio de dispositivos que no pertenecen a la organización.

2. Alcance de la política

Este documento se aplica a todos los dispositivos personales, de colaboradores o terceros que son conectados a la red y/o infraestructura de Techcore, que tienen la capacidad de almacenar, transferir y/o procesar cualquier tipo de información sensible dentro el alcance del Sistema de gestión de seguridad de la información (SGSI). Entre estos dispositivos se incluyen a laptops, PC de escritorios, teléfonos inteligentes, unidades de memoria USB, cámaras digitales, etc. En esta política se les dará el tratamiento a estos dispositivos como BYOD.

3. Usuarios a los que aplica esta política

Esta política aplica a todos colaboradores de Techcore y/o terceros que colaboren con Techcore.

4. Documentos de referencia

Norma ISO/IEC 27001, puntos A.6.2.1, A.6.2.2, A.13.2.1

5. Políticas para el uso de dispositivos BYOD

Las políticas presentes en este documento aplican para todos los BYOD, ya sea de uso personal o que se utilicen para trabajar de forma presencial o remota, dentro o fuera de las instalaciones de Techcore.

5.1 Política de Techcore para BYOD

Los datos de la compañía que se almacenan transfieren o se procesan en BYOD siguen perteneciendo a Techcore, y Techcore mantiene el derecho a controlar esos datos, aunque Techcore no sea el propietaria del dispositivo.

5.2 Quien tiene permitido utilizar BOYD

La alta gerencia de Techcore listara y aprobara los cargos y/o personas a quienes se les permite utilizar BOYD así como también las aplicaciones y bases de datos a las cuales pueden acceder los colaboradores y/o terceros con sus propios dispositivos.

5.3 Uso aceptable de BYOD

Lo siguiente es obligatorio para todos los BYOD:

1. Los dispositivos BYOD deben tener el software de antivirus instalado con su debida licencia y actualizado a la fecha.
2. Cuando un colaborador o asociado utilice dispositivos BYOD estos deberán alinearse a las políticas de contraseñas establecidas por Techcore.
3. Cuando se utilicen BYOD fuera de las instalaciones de Techcore, no deben ser dejados desatendidos y, si es posible, deben estar físicamente resguardados.
4. Cuando los dispositivos BYOD se utilicen en lugares de terceros, el propietario debe tener la precaución de que los datos de Techcore no puedan ser leídos por personas no autorizadas.
5. Se deben instalar periódicamente parches y actualizaciones.
6. La información clasificada debe contar con protección adicional de acuerdo con la Política de Clasificación de la información.

No se permite hacer lo siguiente con los dispositivos BYOD:

1. Permitir el acceso al dispositivo a cualquier persona que no tenga una relación actual con Techcore.
 2. Almacenar material ilegal en el dispositivo.
 3. Instalar software sin licencia.
 4. Conectarse por Bluetooth con cualquier tipo de dispositivo.
 5. Conectarse a redes Wi-Fi desconocidas.
 6. Almacenar claves localmente aplicaciones o servicios de la compañía y clientes.
 7. Transferir datos de la empresa a otros dispositivos no permitidos.
1. Derechos otorgados por el dueño del BYOD a Techcore

Techcore tiene el derecho de ver, editar y borrar todos los datos de la empresa que se encuentran almacenados, transferidos o procesados en BYOD. Techcore está autorizado a configurar cualquier BYOD en conformidad con la presente política y a controlar su uso a través los protocolos de seguridad establecidos. Techcore tiene el derecho de realizar el borrado completo de todos los datos de la compañía que haya en el BYOD si considera que es necesario para la protección de los datos de la empresa, sin el consentimiento del propietario del dispositivo.

5.4 Violaciones de seguridad

Todas las violaciones de seguridad relacionadas con BYOD deben ser reportadas inmediatamente Techcore.