POLÍTICA TRAE TU PROPIO DISPOSITIVO (BYOD)

Versión 1.0
7. Apoyo

Código:	POL-07/015/V1.0-Política trae tu propio dispositivo (Byod)
Versión:	1.0
Fecha de emisión:	2025
Creador por:	Depto. Seguridad de la Información
Responsable:	Coordinación del SGSI
Revisión	Anual o ante cambios regulatorios
Nivel de Confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
28-may-25	1.0	Coordinación del SGSI	Creación de documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir cómo EthicsGlobal retendrá el control sobre su información mientras se accede a dicha información a través de dispositivos que no pertenecen a la organización.

Este documento se aplica a todos los dispositivos personales que tienen la capacidad de almacenar, transferir o procesar cualquier tipo de información sensible dentro el alcance del Sistema de Gestión de Seguridad de la Información (SGSI). Entre estos dispositivos se incluye a los ordenadores personales, teléfonos inteligentes, unidades de memoria USB, cámaras digitales, etc. En esta política se identificará a estos dispositivos como BYOD.

Los usuarios de este documento son todos los empleados de EthicsGlobal.

2. Documentos de referencia

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

3. Reglas de seguridad para el uso de BYOD

Las reglas de la presente Política aplican para todos los BYOD, ya sea de uso personal o que se utilicen para trabajar, dentro o fuera de las instalaciones de la organización.

3.1. Política de la empresa

EthicsGlobal acota el uso de BOYD solamente a una cantidad limitada de empleados que, de otra forma, no podrían realizar su trabajo.
Los datos de la empresa que se almacenan, transfieren o procesan en BOYD siguen perteneciendo a la empresa, y la empresa mantiene el derecho a controlar esos datos aunque no sea propietaria del dispositivo.
Los teléfonos móviles personales de empleados o visitantes que se conecten a la red de invitados no son considerados en el ámbito de ésta política.

3.2. Quiénes pueden utilizar BOYD y para qué

El Coordinador del SGSI creará una lista de cargos y/o personas a quienes se les permite utilizar BOYD junto con las aplicaciones y bases de datos a las cuales pueden acceder con sus propios dispositivos.
El Coordinador del SGSI creará una lista de aplicaciones prohibidas para BOYD.

3.3. Qué dispositivos están permitidos

El Coordinador de SGSI creará una Lista de dispositivos aceptados que pueden ser utilizados como BOYD, junto con configuraciones obligatorias para cada dispositivo.

3.4. Uso aceptable

Lo siguiente es obligatorio para todos los BOYD:

• No se realizarán copias de seguridad de los BYOD ya que no serán generadores de información sino sólo consumirán.

• El método de autenticación será contraseña del Sistema Operativo.

• Los BYOD sólo podrán hacer uso de la red de invitados de EthicsGlobal.

• Cuando se utilicen BOYD fuera de las instalaciones de la empresa, no deben ser dejados desatendidos y, si es posible, deben estar físicamente resguardados bajo llave.

• Cuando se utiliza BOYD en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.

• Se deben instalar periódicamente parches y actualizaciones.

• La información clasificada debe contar con protección adicional de acuerdo con la Política de Clasificación de la Información.

• Notificar al Coordinador del SGSI antes de eliminar, vender o entregar un BOYD a terceros para su reparación.

No se permite hacer lo siguiente con los BOYD:

• Permitir el acceso a cualquiera que no sea el empleado propietario del dispositivo.

• Instalar aplicaciones que están enumeradas en la Lista de aplicaciones prohibidas para BOYD.

• Almacenar material ilegal en el dispositivo.

• Instalar software sin licencia.

• Conectarse por Bluetooth con cualquier tipo de dispositivo.

• Conectarse a redes Wi-Fi desconocidas.

• Almacenar localmente la siguiente información: Llaves privadas de EthicsGlobal.

• Transferir datos de la empresa a otros dispositivos no permitidos.

3.5. Derechos especiales

EthicsGlobal tiene el derecho de ver, editar y borrar todos los datos de la empresa que se encuentran almacenados, transferidos o procesados en BOYD.
El Coordinador del SGSI está autorizado a configurar cualquier BOYD en conformidad con la presente política y a controlar su uso a través de cualquier tecnología disponible para tal propósito.
EthicsGlobal tiene el derecho de realizar el borrado completo de todos los datos de EthicsGlobal del BYOD si considera que es necesario para la protección de los datos de la empresa, sin el consentimiento del propietario del dispositivo.

3.6. Reembolso

EthicsGlobal no abonará a los empleados (los propietarios de BYOD) ningún costo por el uso del dispositivo con fines laborales.

EthicsGlobal abonará lo siguiente:

• Todo nuevo software que necesite ser instalado para uso de la empresa.

• El uso de los datos móviles por concepto de trabajo.

3.7. Violaciones de seguridad

Todas las violaciones de seguridad relacionadas con BOYD deben ser reportadas inmediatamente al Coordinador del SGSI. Además, todas las debilidades que aún no se hayan convertido en incidentes deben ser reportados por medio de los mismos canales dentro de 1 día hábil.

3.8. Capacitación y concienciación

El Coordinador del SGSI está a cargo de la capacitación de los empleados nuevos y existentes sobre el uso adecuado de los BOYD, como también de concientizar sobre las amenazas más comunes.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Lista de usuarios habilitados para BOYD y a qué pueden acceder SGSI-BYODUsers.xlsx	Carpeta de compartida	Coordinador del SGSI	Solamente el Coordinador del SGSI puede editar y publicar nuevas versiones de la Lista.	La lista que ya no tiene validez debe ser archivada por 3 años.
Lista de dispositivos BOYD aceptados y sus configuraciones SGSI-BYODDevices.xlsx	Carpeta de compartida	Coordinador del SGSI	Solamente el Coordinador del SGSI puede editar y publicar nuevas versiones de la Lista.	La lista que ya no tiene validez debe ser archivada por 3 años.
Lista de aplicaciones prohibidas para BOYD SGSI-BYODForbiddenApplications.xlsx	Carpeta de compartida	Coordinador del SGSI	Solamente el Coordinador del SGSI puede editar y publicar nuevas versiones de la Lista.	La lista que ya no tiene validez debe ser archivada por 3 años.

5. Validez y gestión de documentos

Esta política será revisada anualmente por el Comité de Seguridad de la Información o, cuando ocurra un cambio significativo en los roles organizacionales.

El propietario de este documento es el Coordinador del SGSI, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año. El Coordinador del SGSI revisará la Lista de usuarios habilitados, la Lista de dispositivos aceptados y la Lista aplicaciones prohibidas cada 3 meses.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:
• Cantidad de incidentes relacionados con el uso de BOYD.
• Cantidad de empleados que utilizan BOYD sin autorización.

Representante de la Dirección General
Liuva Anahí Figueroa Gracián