POLÍTICA DE TRAE TU PROPIO DISPOSITIVO (BYOD)	PRO-10
	Revisión 00

REV.	FECHA	DESCRIPCIÓN

ELABORADO POR: Carlos J. Pérez Aguilera	REVISADO Y APROBADO POR: DIRECCIÓN
FECHA: 05/05/2018	

POLÍTICA DE TRAE TU PROPIO DISPOSITIVO (BYOD)	PRO-10
	Revisión 00

ÍNDICE

1.-OBJETO

POLÍTICA DE TRAE TU PROPIO DISPOSITIVO (BYOD)	PRO-10
	Revisión 00

El objetivo de este documento es definir cómo la empresa 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. 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

2.-ALCANCE

Este procedimiento es aplicable a todo el personal de la empresa.

3.-DEFINICIONES

No aplica

4.- 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.

4.1. Política de la empresa

La empresa acota el uso de BYOD 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 BYOD siguen perteneciendo a la empresa, y la empresa mantiene el derecho a controlar esos datos, aunque no sea propietaria del dispositivo.

4.2. Quiénes pueden utilizar BYOD y para qué

POLÍTICA DE TRAE TU PROPIO DISPOSITIVO (BYOD)	PRO-10
	Revisión 00

El Responsable de Seguridad creará una Lista de cargos y/o personas a quienes se les permite utilizar BYOD junto con las aplicaciones y bases de datos a las cuales pueden acceder con sus propios dispositivos.

El Responsable de Seguridad creará una lista de aplicaciones prohibidas para BYOD.

4.3. Qué dispositivos están permitidos

El Responsable de Seguridad creará una Lista de dispositivos aceptados que pueden ser utilizados como BYOD, junto con configuraciones obligatorias para cada dispositivo (Por ejemplo, cortafuegos, copias de seguridad, bloqueo de pantalla, etc.)

4.4. Uso aceptable

Lo siguiente es obligatorio para todos los BYOD:

- Deben realizarse copias de seguridad diarias de la empresa contenida en los BYOD
- Todos los BYOD deben tener instalado software antivirus, y en la medida de lo posible, software de prevención de intrusiones (malware), software para administración de dispositivos móviles, etc.
- Cuando sea posible, la información de la empresa estará encriptada en los dispositivos BYOD
- Los dispositivos BYOD deberán estar protegidos mediante métodos de autenticación como, por ejemplo, claves, contraseñas, lectores biométricos, etc.
- El contenido de la empresa no estará compartido para ningún tipo de redes o usuarios (excepto dentro de la intranet de la empresa) o solo podrán compartirse mediante algún método seguro de conexión a la red de la empresa, por ejemplo, VPN.
- Cuando se utilicen BYOD 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 BYOD 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 Responsable de Seguridad antes de eliminar, vender o entregar un BYOD a terceros para su reparación.

No se permite hacer lo siguiente con los BYOD:

- 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 BYOD. 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 claves localmente
- Almacenar localmente información de datos personales
- Transferir datos de la empresa a otros dispositivos no permitidos.

4.5. Derechos especiales

O.F.G tiene el derecho de ver, editar y borrar todos los datos de la empresa que se encuentran almacenados, transferidos o procesados en BYOD.

El Responsable de Seguridad está autorizado a configurar cualquier BYOD en conformidad con la presente política y a controlar su uso a través de algún software para gestión de dispositivos móviles.

O.F.G tiene el derecho de realizar el borrado completo de todos los datos de la empresa 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.

4.6. Reembolso

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

O.F.G abonará lo siguiente:

- Todo nuevo software que necesite ser instalado para uso de la empresa.
- Costos de telecomunicaciones (cargos de teléfono y datos) si puede definirse el porcentaje de uso para la empresa de las facturas mensuales del propietario.

4.7. Violaciones de seguridad

Todas las violaciones de seguridad relacionadas con BYOD deben ser reportadas inmediatamente al Responsable de Seguridad. 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.

4.8. Capacitación y concienciación

El Responsable de Seguridad está a cargo de la capacitación de los empleados nuevos y existentes sobre el uso adecuado de los BYOD, como también de concientizar sobre las amenazas más comunes.

-ARCHIVO Y CODIFICACIÓN DE REGISTROS

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Lista de usuarios habilitados para BYOD y a qué pueden acceder	Carpeta RGPD	Resp. Seguridad	Solamente el Responsable de Seguridad 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 BYOD aceptados y sus configuraciones	Carpeta RGPD	Resp. Seguridad	Solamente el Responsable de Seguridad 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 BYOD	Carpeta RGPD	Resp. Seguridad	Solamente el Responsable de Seguridad puede editar y publicar nuevas versiones de la Lista.	La lista que ya no tiene validez debe ser archivada por 3 años.