



# **USO DE DISPOSITIVOS INTELIGENTES EN ZONA OPERATIVA**

**PO.SGSI.PDI.01**

**Versión 1.0**

## 1. OBJETIVO

Dar a conocer los lineamientos para la solicitud, autorización, uso y retiro del permiso de dispositivos inteligentes en zonas operativas y/o accesos restringidos, con el fin de proteger la información confidencial y garantizar el cumplimiento en las políticas normativas e internas de seguridad de la información de Pentafon.

## 2. ALCANCE

Aplica a todo el personal Directivo, Gerencial, Coordinación, personal operativo y cualquier colaborador que requiera el uso de un dispositivo inteligente dentro de las zonas operativas de Pentafon.

Entendiéndose por dispositivo inteligente todo equipo telefónico, tableta, reloj inteligente, entre otros.

## 3. RESPONSABLES

| Rol                              | Responsabilidad                                                                                                                                         |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Director/ Gerente / Coordinador  | Solicitar autorización para el uso del dispositivo inteligente (teléfono celular) especificando campaña, justificación y periodo de uso.                |
| Seguridad de la Información      | Evaluar la solicitud, autorizar el uso, gestionar la firma de responsiva y comunicar a ADP (Área de control de accesos) el listado de permisos activos. |
| ADP (Área de control de accesos) | Validar los listados autorizados, emitir credenciales de permiso y administrar el retiro cuando corresponda.                                            |

## 4. LINEAMIENTOS

### 4.1 SOLICITUD DE PERMISO DE DISPOSITIVO INTELIGENTE (TELÉFONO CELULAR)

El Gerente y/o Coordinador debe enviar una solicitud formal por *correo electrónico*: [seguridad@pentafon.com](mailto:seguridad@pentafon.com) al área de Seguridad de la Información, indicando los siguientes puntos:

- Nombre completo del colaborador
- Numero de empleado
- Puesto
- Campaña a la que pertenece.
- Justificación del uso del teléfono celular
- Temporalidad del permiso solicitado

**Excepciones:**

- En el caso de Directores, Subdirectores y Gerentes; el equipo de Cultura que lleva el Onboarding deberá gestionar la emisión del permiso del celular. El cual deberá acudir a la firmar de la Responsiva de Uso de Teléfono Celular y notificará a ADP (Área de control de accesos) que se encuentra dentro del listado del permiso, para la impresión de la credencial.
- Directores y/o Gerentes deberán firmar la responsiva de uso de smartwatch, pero solo aquellos que su ofician este en operación, los demás no deberán ingresarlo.

**Importante:** En caso de no cumplir con estos datos no se podrá brindar la autorización.

## 4.2 REVISIÓN Y AUTORIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Seguridad de la Información evalúa la solicitud para determinar la necesidad operativa del dispositivo. En caso de aprobación, solicita que el colaborador acuda a firmar la Responsiva de Uso de Teléfono Celular.

## 4.3 FIRMA DE LA RESPONSIVA

El colaborador acude al área de Seguridad de la Información a firmar la Responsiva de Uso de Teléfono Móvil, en la cual se compromete a:

- Mantener bajo resguardo su teléfono móvil dentro de las instalaciones (no dejarlo en abandono).
- No fotografiar operaciones, documentos, pantallas, ni ningún elemento que contenga información sensible de PentaFon. (PO.SGSI.PRS.01)
- Evitar que su teléfono móvil sea utilizado por terceros.
- Utilizar el teléfono únicamente en el área autorizada, misma que declara conocer.
- Notificar a Seguridad de la Información cualquier cambio de equipo telefónico el mismo día de su ingreso con un dispositivo distinto.
- No ingresar con smartwatch, audífonos o cualquier dispositivo vinculado al teléfono móvil.

## 4.4 COMUNICACIÓN A ADP

Seguridad de la Información envía un correo electrónico a ADP con el listado actualizado del personal autorizado con permiso para uso de celular, una vez que el colaborador haya firmado la responsiva.

## 4.5 VALIDACIÓN DE ADP

ADP valida el listado de personal autorizado y confirma la recepción y revisión de la información.

#### 4.6 EMISIÓN DE CREDENCIAL DE PERMISO

ADP (Área de control de accesos) imprime y entrega al colaborador la Credencial de Permiso de Uso de Teléfono Celular, que deberá portar visiblemente durante su jornada laboral. En el caso de Directores y Subdirectores, ADP (Área de control de accesos) emite el permiso directamente tras recibir la notificación de Seguridad de la Información.

#### RETIRO DE PERMISO DE DISPOSITIVO INTELIGENTE (TELÉFONO CELULAR)

##### 4.7 SOLICITUD DE RETIRO

El jefe Directo envía un correo electrónico Seguridad de la Información y a ADP (Área de control de accesos) solicitando el retiro del permiso de celular por alguno de los siguientes motivos:

- Cambio de campaña.
- No acreditó el training y regresa a su posición inicial.
- Finalización de temporalidad del permiso.
- Incumplimiento de las políticas de uso.

##### 4.8 VALIDACIÓN POR SEGURIDAD DE LA INFORMACIÓN

Seguridad de la Información revisa y valida la solicitud de retiro, confirmando por correo electrónico la revocación del permiso.

##### 4.9 RETIRO DE CREDENCIAL

ADP (Área de control de accesos) recibe la confirmación, retira la credencial de permiso al colaborador y notifica por correo electrónico la finalización del permiso.

#### 5. REFERENCIAS

- Norma ISO 9001:2015 Sistemas de Gestión de la Calidad – Requisitos NMX-CC-9001-IMNC-2015.
- Norma ISO 27001:2022 Sistemas de Gestión de Seguridad de la información.
- Modelo Global CIC.
- Norma ISO 18295-1:2017 Centros de contacto con el cliente.

## 6. CONTROL DE CAMBIOS

| Actualización                | Fecha      | Responsable    | Versión |
|------------------------------|------------|----------------|---------|
| I. Elaboración del documento | 13 10 2025 | Vanessa Romero | 1.0     |

## 7. AUTORIZACIÓN

| Elaboró           | Revisó                   | Revisó                              | Autorizó              |
|-------------------|--------------------------|-------------------------------------|-----------------------|
| Areli Luna        | Vanessa Romero           | Angelica Hernandez                  | Edmundo Olguín        |
| <i>Auditor SI</i> | <i>Subdirectora CISO</i> | <i>Gerente Relaciones Laborales</i> | <i>Director de TI</i> |