EMPLEADOS

Uso de dispositivos móviles no corporativos

básico

Normas y procedimientos BYOD.

Elaboras normas y procedimientos específicos si permites BYOD en tu empresa (usos permitidos, antivirus, actualización, configuraciones,…)

Prohibición de uso de dispositivos manipulados.

Prohíbes el uso de dispositivos rooteados o a los que se ha realizado jailbreak.

Concienciación de los empleados.

Involucras a los usuarios en la protección de sus propios dispositivos y de los datos que contienen o a los que pueden acceder.

Formación de los empleados.

Proporcionas a tus empleados charlas o formación sobre cómo proteger sus dispositivos (contraseñas, actualizaciones, permisos, etc.).

Limitar el acceso a redes externas.

Prohíbes el uso de redes inalámbricas externas no corporativas salvo 3G/4G.

Lista de aplicaciones no permitidas.

Mantienes una lista de aplicaciones no permitidas y la difundes entre tus empleados.

Controlar el almacenamiento en la nube de datos corporativos.

Supervisas el uso de aplicaciones de almacenamiento en la nube.

Proceso de borrado de la información.

Aplicas una normativa de entrega/eliminación de la información de sus dispositivos cuando el empleado abandona la empresa.

Control de usuarios y dispositivos.

Mantienes un registro actualizado con usuarios, dispositivos y privilegios de acceso.

protege tu empresa

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

EMPLEADOS

Uso de dispositivos móviles no corporativos

básico

Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos.

Instalas y configuras medidas para el almacenamiento seguro a la información (clasificación de información, cifrado de datos, etc.)

Bloqueo programado.

Configuras el bloqueo automático del dispositivo tras un periodo de inactividad.

Desconexión wifi y Bluethooth.

Desactivas en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no son necesarios.

Cumplimiento de la normativa.

Conoces y aceptas la normativa corporativa vigente para el uso de tus dispositivos en actividades de la empresa.

avanzado

Control de acceso a la red.

Implementas un control de acceso (autenticación con contraseñas, doble factor, VPN…) a la red corporativa desde estos dispositivos.

Extravío de dispositivos.

Configuras medidas de seguridad para proteger la información corporativa en los dispositivos (localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas) en caso de extravío.