POLÍTICA DE USO DE DISPOSITIVOS PARA MOVILIDAD EN LA FGUV

Versión:	**2**
Fecha de la versión:	**21-03-2020**
Creado por:	**Departamento Jurídico y Departamento informática**
Aprobado por:	**Gerencia**
Nivel de confidencialidad:	**USO INTERNO**

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
23/07/2019	1	Jurídico/Informática	POLÍTICA DE USO DE DISPOSITIVOS PARA MOVILIDAD Anexo 9 Medidas técnicas disponibles en el punto 5.3. 6 de la intranet de la FGUV
21/03/2020	2	Jurídico/Informática	Adaptación a las medidas excepcionales derivadas de la emergencia sanitaria

Índice

1. INTRODUCCIÓN

Cuando el puesto de trabajo lo requiere, la FGUV concede al personal la posibilidad de utilizar teléfonos inteligentes, tabletas y/o portátiles de la FGUV y/o utilizar dispositivos propios para uso laboral conectados a la red.

La FGUV se reserva el derecho de revocar esta posibilidad si las personas usuarias no cumpliesen con las políticas y procedimientos descritos a continuación.

Esta política tiene por objeto proteger la seguridad e integridad de la información y de los datos de la FGUV o los gestionados por ésta.

2. USO DE DISPOSITIVOS PRIVADOS

Se adoptarán las siguientes medidas:

- Evitar que terceros ajenos a la organización (familiares) accedan a la información de la FGUV.
- Tener un antivirus instalado y actualizado.
- Crear una cuenta de usuario distinta de la personal.
- Disponer de contraseñas seguras y no compartirlas.
- Cumplir con todas las medidas de seguridad que deben aplicar en las instalaciones de la FGUV como son:
  - ✓ Activar los bloqueos de pantalla por inactividad.
  - ✓ Cerrar las sesiones de trabajo cuando abandonen su puesto de trabajo en su domicilio.
  - ✓ Si se trabaja con documentos en papel, custodiarlos bajo llave.

- ✓ Si tienen alguna incidencia de seguridad comunicarlo inmediatamente al departamento de informática.
- ✓ No utilizar redes públicas
- ✓ Mantener los dispositivos actualizados
- ✓ Eliminar información temporal que se haya podido almacenar en las carpetas de descarga, papelera de reciclaje, mis documentos.
- ✓ Borrar el histórico de navegación, las cookies.
- ✓ No guardar contraseñas.

3. INSTALACIÓN DE APLICACIONES

Se debe verificar la seguridad de las aplicaciones instaladas en los dispositivos. Consultar al departamento de informática en caso de duda.

4. CONTRASEÑAS

- Con el fin de evitar el acceso no autorizado, los dispositivos deben ser protegidos con contraseña usando las características del dispositivo, así como una contraseña fuerte para acceder a la red de la FGUV.

- Las contraseñas deben tener al menos seis caracteres y una combinación de letras mayúsculas y minúsculas, números y símbolos. Las contraseñas se cambiarán mínimo una vez al año y la nueva contraseña no puede ser una de las contraseñas anteriores.

- El dispositivo se tiene que bloquear con una contraseña o PIN si está inactivo durante cinco minutos.

- Después de cinco intentos fallidos de inicio de sesión, el dispositivo se bloqueará.

- Los dispositivos crackeados (por ejemplo, jailbreak) tienen estrictamente prohibido el acceso a la red.

- Smartphones, tabletas y portátiles que pertenecen al personal que se utilicen para uso corporativo, rigen las mismas normas de seguridad establecidas en el presente documento.

- El acceso de los empleados a los datos de la FGUV se limita a base de perfiles definidos por el departamento de informática y ejecutado automáticamente.

5. RESPONSABILIDADES

- Aunque se tomarán todas las precauciones para evitar que los datos personales del personal se pierdan en caso de borrado remoto de un dispositivo, es responsabilidad del personal tomar precauciones adicionales, como copias de seguridad de correo electrónico, contactos, etc.

- La FGUV se reserva el derecho de desconectar los dispositivos o desactivar los servicios en caso de robo/pérdida o problema de seguridad grave.

- El personal deberá usar los dispositivos de manera ética en todo momento.

- El personal asume la total responsabilidad por los riesgos, incluyendo, pero no limitado a la pérdida parcial o total de los datos personales debido a un fallo del sistema operativo errores, virus, programas maliciosos y / u otras fallas de software o hardware, o la programación errores que hacen que el dispositivo inutilizable.

6. INCIDENCIAS DE SEGURIDAD

El personal que tenga conocimiento de una incidencia de seguridad es responsable de la comunicación inmediata de la misma a los teléfonos 963531064 o 963531072 así como enviar un correo electrónico a informatica.fguv@uv.es explicando lo sucedido.

La pérdida o robo de dispositivos deben ser comunicadas a la FGUV dentro de las 24 horas siguientes. El personal es responsable de notificar a su compañía de telefonía móvil inmediatamente después de la pérdida de un dispositivo propio.

Una incidencia es cualquier evento que a juicio del usuario pueda poner en riesgo el sistema de información. Serán consideradas como incidencias, entre otras, la pérdida y/o robo del dispositivo.

7. INCUMPLIMIENTO

La FGUV se reserva el derecho de tomar las medidas disciplinarias apropiadas, conforme a lo establecido en el convenio colectivo, y en base al incumplimiento de esta política.

CRISTOBAL JOSE|SURIA|LUENGO
Firmado digitalmente por CRISTOBAL JOSE|SURIA|LUENGO
Fecha: 2020.03.22 19:38:07 +01'00'