

MUNICIPALIDAD PROVINCIAL DE CORONEL PORTILLO
OFICINA DE TECNOLOGIAS DE LA INFORMACION

NORMA DE SEGURIDAD EN EQUIPOS MÓVILES

  PUCALLPA MUNICIPALIDAD PROVINCIAL DE CORONEL PORTILLO	DOCUMENTO:	
	NORMA DE SEGURIDAD EN EQUIPOS MÓVILES	
	CÓDIGO: NO-015	EDICIÓN: 01 FECHA APROBACIÓN: 30/11/2014

1. Objetivo

Garantizar que no se comprometa la información de Municipalidad Provincial de Coronel Portillo, en adelante la MPCP, cuando se utilizan dispositivos informáticos móviles.

2. Disposiciones Generales

Se tienen definidas las siguientes responsabilidades:

2.1. La OTI es responsable de:

- Otorgar los permisos de acceso a la red de la MPCP, para los equipos móviles de terceros, en caso se requiera.
- Autorizar el ingreso a las instalaciones de la MPCP de equipos móviles de terceros, ya sean proveedores, consultores, auditores externos o equipos personales de los colaboradores.

2.2. El Encargado de Seguridad de la OTI es responsable de:

- Asegurar que el equipo móvil de terceros no representa riesgo alguno o que no pone en riesgo la integridad de los datos de la MPCP y sistemas que los soportan.

2.3. La OTI es responsable de:

- Configurar los equipos móviles de terceros con el fin de alinearlos a los estándares de seguridad de la MPCP y de esta forma puedan ingresar de forma segura a la red.

3. Descripción

- 3.1. Cuando se utilizan dispositivos informáticos móviles tales como computadoras personales, organizadores y/o teléfonos móviles, se debe tener especial cuidado en garantizar que no se comprometa la información de la MPCP. Se debe tomar en cuenta los riesgos que implica trabajar con herramientas informáticas móviles en particular en ambientes no protegidos. Dentro de estas consideraciones debe incluirse los requerimientos de protección física, controles de acceso, técnicas criptográficas, resguardos y protección contra virus. Debe incluirse además reglas y asesoramiento en materia de conexión de dispositivos móviles a redes y orientación sobre uso de estos dispositivos en lugares públicos.
- 3.2. Se deben tomar consideraciones al utilizar dispositivos informáticos móviles en lugares públicos, salas de reuniones y otras áreas no protegidas fuera de la sede de la organización. Se debe implementar protección para evitar el acceso no autorizado a la información almacenada y procesada por estas herramientas, o la divulgación de la misma, por ejemplo, mediante técnicas criptográficas.
- 3.3. Es importante que cuando dichos dispositivos sean utilizados en lugares públicos se tomen consideraciones para evitar el riesgo de que la información que aparece en pantalla, sea vista por personas no autorizadas. Se debe implementar procedimientos contra software malicioso y estos deben mantenerse actualizados. El equipamiento debe estar disponible para permitir un procedimiento de resguardo rápido y fácil de la información. Estos procedimientos deben estar adecuadamente protegidos contra situaciones como robo o pérdida de la información.
- 3.4. Se debe brindar protección adecuada para el uso de dispositivos móviles conectados a redes. El acceso remoto a la información de la MPCP a través de redes públicas, utilizando herramientas informáticas móviles, sólo debe tener lugar después de una identificación y autenticación exitosa y con mecanismos adecuados de control de acceso.

  PUCALLPA MUNICIPALIDAD PROVINCIAL DE CORONEL PORTILLO	DOCUMENTO:	
	NORMA DE SEGURIDAD EN EQUIPOS MÓVILES	
	CÓDIGO: NO-015	EDICIÓN: 01 FECHA APROBACIÓN: 30/11/2014

DE LA SEGURIDAD FISICA DE LOS EQUIPOS MÓVILES

- 3.5. Los dispositivos informáticos móviles también deben estar físicamente protegidos contra robo. El equipamiento que transporta información importante de la MPCP, sensible y/o crítica no debe dejarse desatendido; cuando resulte posible debe estar físicamente resguardado bajo llave, o debe utilizarse cadenas de escritorio preferiblemente con llave, ya que las que utilizan clave pueden ser decodificadas.
- 3.6. Se debe brindar entrenamiento al personal que utiliza equipos móviles para incrementar su conocimiento de los riesgos adicionales ocasionados por esta forma de trabajo y de los controles que se deben implementar.

DE LA SEGURIDAD DE LOS EQUIPOS MÓVILES FUERA DE LAS INSTALACIONES DE LA MPCP

- 3.7. El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la organización debe ser autorizado por la MPCP. La seguridad implementada debe ser equivalente a la suministrada dentro de la organización teniendo en cuenta los riesgos de trabajar fuera de la misma. El equipamiento de procesamiento de la información incluye todo tipo de computadoras personales, organizadores, teléfonos móviles, papel u otros formularios, necesarios para el trabajo en el domicilio o que es transportado fuera del lugar habitual de trabajo.
- 3.8. Se debe considerar los siguientes lineamientos:
- El equipamiento y dispositivos retirados del ámbito de la organización no deben permanecer desatendidos en lugares públicos. Las computadoras personales deben ser transportadas como equipaje de mano.
 - Se deben respetar permanentemente las instrucciones del fabricante como la protección por exposición a campos electromagnéticos fuertes.
 - Los controles de trabajo fuera de la institución deben ser determinados a partir de un análisis de riesgo y se aplicará controles adecuados según corresponda, como por ejemplo, gabinetes de archivo con cerradura, política de escritorios limpios y control de acceso a computadoras.
 - Una adecuada cobertura de seguro debe estar en orden para proteger el equipamiento dentro y fuera del ámbito de la organización.
- 3.9. Los riesgos de seguridad tales como robo o interceptación de información pueden variar considerablemente según las ubicaciones y deben ser tenidas en cuenta al determinar los controles más apropiados.

DE LA CONEXIÓN DE EQUIPOS MÓVILES DE TERCEROS A LA RED DE SES

- 3.10. Los equipos de terceros que deban ser conectados a la red de la MPCP deberán contar con la aprobación previa del Encargado de Seguridad del área correspondiente.
- 3.11. Todo equipo de terceros a ser conectado a la red de la MPCP deberá ser revisado para comprobar que cuente con un sistema antivirus actualizado. De no ser así la Oficina de Informática se encargará de notificar al tercero la necesidad de instalar el antivirus necesario.
- 3.12. Se deberá verificar que el sistema operativo cuente con las últimas actualizaciones publicadas por el fabricante.
- 3.13. Se deberá asignar un perfil para la persona que utilizará el equipo considerando las restricciones a los recursos de red.

	DOCUMENTO: NORMA DE SEGURIDAD EN EQUIPOS MÓVILES	
	CÓDIGO: NO-015	EDICIÓN: 01
		FECHA APROBACIÓN: 30/11/2014

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución de Gerencia General.