MUNICIPALIDAD PROVINCIAL DE CORONEL PORTILLO

OFICINA DE TECNOLOGIAS DE LA INFORMACION

NORMA DE SEGURIDAD EN LA RED

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados
01	15/10/2014	Ing. Teofilo Pastor Perez Lazo	Versión Inicial
01	31/10/2014		

1. Objetivo

Minimizar el riesgo del uso no apropiado de la red, servicios y recursos de red de Municipalidad Provincial de Coronel Portillo ,en adelante LA MPCP.

2. Disposiciones Generales

El Encargado de Seguridad de la Información es responsable de verificar el cumplimiento de lo dispuesto en la presente norma.

3. Descripción

3.1. Se deben implementar controles de acceso para todos los servicios de red que conformen la infraestructura tecnológica de la MPCP.

3.2. Todos los usuarios de la red de la MPCP deben contar con accesos únicamente a los servicios para los que fueron autorizados de alguna forma específica.

3.3. La gestión de accesos a la red, se debe dar de acuerdo a procedimientos de creación, modificación y eliminación de accesos.

3.4. Se debe limitar el acceso hacia la red por parte de los usuarios. Se deben implementar mecanismos como: dominios lógicos separados, implementación de VLANs, evitar recorridos cíclicos ilimitados en la red, puertas de enlace predeterminadas, entre otros. Así mismo se deberían implantar mecanismos de detección de intentos de intrusión tanto desde la red interna como externa.

3.5. Todo dispositivo que se conecte a la red de la MPCP debe de tener un identificador único con la finalidad de poder identificar los recursos accedidos desde él. Se debe contar con controles en los terminales de modo que no se pueda alterar el identificador único por personal no autorizado. Estos controles deben ser implementados para que operen tanto para conexiones internas o externas.

3.6. Se debe de segregar y segmentar la red con la finalidad de limitar el acceso a los recursos de la red por parte de los usuarios. Una correcta segregación y segmentación permitirá reducir el riesgo de posibles intentos de intrusión hacia los servicios más importantes de la MPCP.

3.7. Se debe tener una descripción detallada de aquellos servicios de red que no pertenecen a la MPCP pero que son usados por el mismo como parte de su infraestructura tecnológica.

3.8. La conexión entre terminales y servidores debe de realizarse a través de una conexión segura con la finalidad de evitar que la información pueda ser alterada o vista por usuarios no autorizados. La información no segura que puede viajar a través de la red debe ser la mínima necesaria para realizar la conexión segura.

3.9. Todos los usuarios que necesiten tener acceso a la red, deben contar con un identificador único. El identificador único no puede ni debe dar a conocer información relacionada a cargos, ubicación o demás datos que podrían dar a conocer datos confidenciales a usuarios no autorizados.

3.10. En caso de existir sistemas de aplicación o software comprado que tenga herramientas que puedan servir para evadir los controles implementados en la red, se debe de restringir su uso. En caso de ser requeridas para funciones propias del negocio, éstas deben contar con autorización la Oficina de Tecnologías de la Información.

3.11. Se debe establecer un umbral de tiempo tras el cual, un equipo desatendido, debe de bloquearse con la finalidad que evitar que éste sea usado por otro usuario. Además se deberá establecer un umbral máximo de conexión para los usuarios, de acuerdo a la criticidad y demanda del servidor.

3.12. Se debe de restringir el horario habilitado para aceptar nuevas conexiones de usuarios a la red, por ejemplo: únicamente durante horario de oficina.

3.13. Todo sistema de aplicación y/o recurso de red que sea considerado sensible debe, de preferencia, ser aislado de la red con la finalidad de restringir su acceso únicamente a los usuarios autorizados. Las aplicaciones sensibles requieren de autorizaciones respectivas para el ingreso al sistema y manipulación de información. Así mismo, el propietario de la información y la sensibilidad de la misma debe quedar documentado.

3.14. Los servidores críticos no deberían incluir ningún tipo de descripción a modo de banner al establecerse la conexión. Además, se deberá restringir el uso de mensajes de error que puedan brindar información sobre la descripción y características del equipo.

3.15. Los servidores deberán limitar la cantidad consecutiva de intentos errados de conexión, además de llevar internamente en el sistema un registro de dichos eventos.

3.16. Se deberá configurar internamente en los servidores críticos el registro de pistas de auditoría de eventos correspondientes a:

- Accesos exitosos.
- Intentos de conexión fallidos.
- Operaciones críticas.
- Revisión de pistas de auditoría.

4. Vigencia

Entrará en vigencia a partir de su aprobación.

5. Aprobación

Será aprobada mediante Resolución de Gerencia General.