

# Novedades Técnicas en .CL

José Urzúa

[jose@nic.cl](mailto:jose@nic.cl)

# Sitio web

- Pruebas de seguridad
- Pruebas con clientes finales
  - Invitación para realizar pruebas a 100 clientes
- Lanzamiento en paralelo a sitio actual
  - Sitio actual seguirá visible en [www.nic.cl](http://www.nic.cl)
  - Transcurrido periodo de confianza nuevo sitio será visible en [www.nic.cl](http://www.nic.cl)
  - Quedará disponible un acceso para usar sitio antiguo
  - Deshabilitar sitio antiguo

# Segundo Factor de Autenticación

- Se usará para proteger el acceso a las cuentas de usuario en “NIC Chile registrar”
- Activación de 2FA será voluntaria y se debe cumplir con:
  - Autenticación con nombre de usuario y contraseña
  - En “edición de perfil” solicitar “activar 2FA”
    - Sistema solicita contraseña, número de teléfono e información de documento de identidad, luego despliega código QR
    - Usuario lee código QR con aplicación OTP (ejemplo: Google Authenticator)
    - Usuario ingresa código generado por aplicación OTP

# Segundo Factor de Autenticación

- Al activar 2FA:
  - Sistema informa 10 **códigos de recuperación** para anular 2FA en caso de pérdida de dispositivo que genera códigos 2FA
  - Estos códigos deben contar con un almacenamiento seguro
- Si el usuario se conectó con su clave y 2FA puede deshabilitar 2FA
  - Debe informar nuevamente contraseña y código 2FA
- Si el usuario pierde acceso a aplicación que genera código 2FA
  - Puede deshabilitar 2FA identificándose con su contraseña y usando un código de recuperación

# Segundo Factor de Autenticación

- Caso complicado:
  - Usuario pierde acceso a la aplicación 2FA y tampoco tiene los códigos de recuperación
  - Se debe identificar con nombre de usuario-contraseña y solicita la desactivación de 2FA
    - Sistema envía email con enlace válido por 24 horas para cancelar solicitud
    - Si no se cancela, área de Atención a Clientes se comunica telefónicamente con el usuario e informa un código
    - Usuario se identifica con usuario-contraseña e informa el código e imagen de su documento de identidad
    - Si se cumplen las validaciones, se desactiva 2FA

# Registry Lock

- Servicio que bloquea modificaciones a los datos del dominio en el registry
- Definiciones en discusión
  - Activación del servicio es solicitada por el contacto administrativo por medio del agente registrador
    - Debe informar los datos necesarios para desbloquear el dominio
  - Para iniciar el desbloqueo, el contacto administrativo envía solicitud por medio del agente registrador
    - Registry inicia procedimiento de desbloqueo que permitirá modificaciones al dominio por N horas y automáticamente se volverá a bloquear

# ¿Preguntas?

José Urzúa  
jose@nic.cl