POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SISTEMA DE RADIO ASOCIACIÓN RADIAL DE COMUNICACIONES SOCIAL DEL ORIENTE ARCOSOR

1. Política General de Seguridad

- **Objetivo**: Proteger la información y los sistemas de la emisora para que solo personas autorizadas tengan acceso y evitar pérdidas de datos.
- **Responsabilidad**: El equipo de la emisora debera asegurarse de que se sigan estas políticas.

2. Política de Contraseñas

- **Objetivo**: Asegurar que las contraseñas sean seguras y difíciles de adivinar.
- **Normas**:
  - Usar contraseñas de al menos 8 caracteres con letras, números y símbolos.
  - Cambiar las contraseñas cada 90 días.
  - No compartir las contraseñas con nadie.

3. Política de Acceso a la Información

- **Objetivo**: Asegurar que solo las personas autorizadas puedan acceder a la información importante.
- **Normas**:
  - Solo se debe dar acceso a la información que necesite cada persona para su trabajo.
  - Se debe llevar un registro de los accesos a sistemas importantes.
  - El acceso debe cancelarse cuando un empleado termine su trabajo o cambie de puesto.

4. Política de Uso de Dispositivos Móviles y USB

- **Objetivo**: Proteger los dispositivos móviles y USB para evitar que se pierdan o sean usados incorrectamente.
- **Normas**:
  - Los dispositivos móviles deben estar protegidos con contraseñas y cifrados.
  - Los USB deben ser escaneados antes de conectarlos a los sistemas de la emisora.

- No se debe guardar información sensible en dispositivos personales sin permiso.

5. Política de Seguridad en Redes

- **Objetivo**: Proteger la red de la emisora para evitar accesos no autorizados o problemas de seguridad.
- **Normas**:
  - Usar firewalls y sistemas de protección para las redes internas.
  - Cifrar la información cuando sea necesario.
  - Proteger el acceso a las redes Wi-Fi de la emisora, cambiando las contraseñas regularmente.

6. Política de Respaldo de Datos

- **Objetivo**: Asegurar que los datos importantes se puedan recuperar en caso de pérdida o daño.
- **Normas**:
  - Realizar copias de seguridad de los datos importantes todos los días.
  - Guardar los respaldos en un lugar seguro.
  - Comprobar regularmente que los respaldos sean válidos y se puedan restaurar.

7. Política de Gestión de Incidentes de Seguridad

- **Objetivo**: Tener un plan para responder rápidamente a cualquier incidente de seguridad, como un ataque o pérdida de datos.
- **Normas**:

  - Reportar cualquier problema de seguridad de inmediato.
  - Investigar los incidentes para entender qué ocurrió y cómo solucionarlo.
  - Tomar acciones para evitar que se repita el incidente.

8. Política de Protección de Datos Personales

- **Objetivo**: Proteger la información personal de empleados, clientes y oyentes.

- **Normas**:
  - Solo recoger la información personal que sea necesaria.
  - Mantener los datos personales de forma segura.
  - Cumplir con las leyes de protección de datos, como la Ley 1581 de 2012 en Colombia.

Procedimientos de Seguridad de la Información

1. Procedimiento para Nuevos Empleados

- **Objetivo**: Asegurarse de que los nuevos empleados tengan acceso seguro a la información que necesitan para su trabajo.
- **Pasos**:
  1. Verificar que el empleado tiene autorización para acceder a los sistemas.
  2. Asignar acceso según su rol y capacitarlo en las políticas de seguridad.
  3. Hacer firmar al empleado un acuerdo de confidencialidad.

2. Procedimiento de Monitoreo de Sistemas

- **Objetivo**: Revisar regularmente los sistemas para detectar problemas de seguridad.
- **Pasos**:
  1. Monitorear los accesos a sistemas críticos y revisar los registros.
  2. Realizar auditorías periódicas para identificar posibles amenazas.
  3. Informar cualquier hallazgo sospechoso y tomar acciones para corregirlo.

3. Procedimiento ante Incidentes de Seguridad

- **Objetivo**: Tener un plan claro para manejar cualquier incidente de seguridad, como un hackeo o pérdida de datos.
- **Pasos**:
  1. Notificar inmediatamente si se detecta un incidente.
  2. Detener cualquier actividad sospechosa y aislar los sistemas afectados.
  3. Investigar lo ocurrido y tomar medidas para prevenir futuros incidentes.

4. Procedimiento de Respaldo y Recuperación

- **Objetivo**: Garantizar que los datos se puedan recuperar en caso de pérdida.
- **Pasos**:

1. Hacer copias de seguridad regulares y mantenerlas seguras.
2. Verificar que las copias de seguridad se pueden restaurar correctamente.
3. Tener un plan de acción claro para restaurar la información en caso de desastre.

5. Procedimiento de Desactivación de Cuentas

- **Objetivo**: Asegurarse de que los accesos de empleados que ya no trabajan en la emisora sean eliminados de inmediato.

- **Pasos**:
  1. Desactivar las cuentas de usuario del empleado cuando deje de trabajar en la emisora.
  2. Recuperar cualquier dispositivo que el empleado haya utilizado.
  3. Verificar que la información sensible esté protegida.

Conclusión

Estas políticas y procedimientos son esenciales para garantizar la seguridad de la información en una emisora pequeña. Proteger los datos y los sistemas no solo evita problemas de seguridad, sino que también asegura la confianza de empleados, clientes y oyentes. Es importante que todos los empleados comprendan y sigan estas políticas para mantener un entorno seguro.