POLITICAS DE SEGURIDAD EN INFORMATICA

Las políticas de seguridad informática son documentos formales que establecen las directrices, procedimientos y medidas que una organización debe seguir para proteger sus sistemas de información y datos. A continuación se describen algunos elementos clave y tipos de políticas de seguridad informática que una organización debe considerar:

1. **Política de Uso Aceptable (AUP)**
   - Definición: Establece las reglas sobre el uso apropiado de los recursos informáticos de la organización.
   - Contenido: Directrices sobre el uso de internet, correo electrónico, software autorizado, y dispositivos personales.
   - Objetivo: Prevenir el uso indebido que pueda comprometer la seguridad o la eficiencia de los sistemas.

2. **Política de Gestión de Contraseñas**
   - Definición: Describe los requisitos para la creación y gestión de contraseñas seguras.
   - Contenido: Longitud mínima, complejidad, frecuencia de cambio, almacenamiento seguro y prohibición de compartir contraseñas.
   - Objetivo: Asegurar que las contraseñas sean difíciles de adivinar o comprometer.

3. **Política de Control de Acceso**
   - Definición: Establece cómo se otorgan, supervisan y revocan los accesos a los sistemas y datos.
   - Contenido: Asignación de roles y permisos, uso de autenticación multifactor, y revisión periódica de accesos.
   - Objetivo: Garantizar que solo las personas autorizadas tengan acceso a recursos específicos.

4. **Política de Respuesta a Incidentes**
   - Definición: Proporciona un plan para identificar, responder y recuperarse de incidentes de seguridad.
   - Contenido: Procedimientos para detectar, reportar, mitigar, y documentar incidentes.
   - Objetivo: Minimizar el impacto de los incidentes de seguridad y recuperar operaciones normales rápidamente.

5. **Política de Copias de Seguridad (Backups)**
   - Definición: Define cómo y cuándo se realizan copias de seguridad de datos críticos.
   - Contenido: Frecuencia de backups, almacenamiento seguro de copias, y procedimientos de restauración.
   - Objetivo: Asegurar la disponibilidad y recuperación de datos en caso de pérdida o corrupción.

6. **Política de Gestión de Parches**
   - Definición: Describe el proceso para la aplicación de parches y actualizaciones de software.
   - Contenido: Evaluación de vulnerabilidades, planificación y despliegue de parches, y verificación post-implementación.
   - Objetivo: Mantener los sistemas actualizados y protegidos contra vulnerabilidades conocidas.

7. **Política de Seguridad de Datos**
   - Definición: Establece cómo se debe proteger la integridad, confidencialidad y disponibilidad de los datos.
   - Contenido: Clasificación de datos, métodos de cifrado, y directrices para el manejo de información sensible.
   - Objetivo: Proteger los datos contra accesos no autorizados y pérdida de información.

8. **Política de Seguridad Física**
   - Definición: Proporciona directrices para la protección física de los activos informáticos.
   - Contenido: Control de acceso a instalaciones, protección contra desastres naturales, y medidas contra robo o vandalismo.
   - Objetivo: Evitar el acceso físico no autorizado y daños a los recursos informáticos.

9. **Política de Seguridad en el Desarrollo de Software**
   - Definición: Define las prácticas seguras a seguir durante el ciclo de vida del desarrollo de software.
   - Contenido: Revisión de código, pruebas de seguridad, y control de versiones.
   - Objetivo: Garantizar que el software desarrollado esté libre de vulnerabilidades.

10. **Política de Formación y Concienciación en Seguridad**
    - Definición: Establece programas de formación y concienciación sobre seguridad para los empleados.
    - Contenido: Planes de formación regular, campañas de concienciación, y evaluación de conocimientos.
    - Objetivo: Aumentar la consciencia de los empleados sobre las amenazas de seguridad y promover prácticas seguras.

11. **Política de Gestión de Riesgos**
    - Definición: Proporciona un marco para la identificación, evaluación y mitigación de riesgos de seguridad.
    - Contenido: Metodologías de análisis de riesgos, evaluación de impacto, y planes de mitigación.
    - Objetivo: Reducir la probabilidad y el impacto de incidentes de seguridad mediante una gestión proactiva de riesgos.

12. **Política de Uso de Dispositivos Móviles**
    - Definición: Establece las directrices para el uso seguro de dispositivos móviles en la organización.
    - Contenido: Requisitos de seguridad para dispositivos, cifrado de datos, y políticas de acceso remoto.
    - Objetivo: Proteger la información de la organización en dispositivos móviles y reducir el riesgo de pérdida o robo.

13. **normativa vigente en materia de seguridad informática y protección de datos personales en Chile**

    Ley N° 19.628 sobre Protección de la Vida Privada
    - Descripción: Esta ley, también conocida como Ley de Protección de Datos Personales, regula el tratamiento de datos personales en Chile.
    - Contenido: Establece principios y obligaciones para el tratamiento de datos personales, derechos de los titulares de los datos, y sanciones en caso de incumplimiento.

- Objetivo: Proteger la privacidad de las personas y regular el tratamiento de sus datos personales.

Ley N° 20.285 sobre Acceso a la Información Pública
- Descripción: Conocida como Ley de Transparencia, regula el derecho de acceso a la información pública y establece las obligaciones de transparencia de los organismos del Estado.
- Contenido: Estipula cómo los ciudadanos pueden acceder a la información pública y cómo las instituciones deben publicar información relevante.
- Objetivo: Promover la transparencia y el acceso a la información en el ámbito público.

Ley N° 19.223 sobre Delitos Informáticos
- Descripción: Esta ley tipifica y sanciona los delitos informáticos en Chile.
- Contenido: Define y penaliza conductas como el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones, la falsificación de datos, y otros delitos relacionados con el uso indebido de tecnologías de la información.
- Objetivo: Proteger los sistemas y datos informáticos contra actividades delictivas.
-

Ley N° 21.096 que crea la Agencia Nacional de Ciberseguridad
- Descripción: Establece la creación de la Agencia Nacional de Ciberseguridad en Chile.
- Contenido: Define las funciones y competencias de la agencia para coordinar y ejecutar políticas de ciberseguridad a nivel nacional.
- Objetivo: Fortalecer la seguridad cibernética en el país a través de una entidad especializada.
-

Decreto Supremo N° 83 del Ministerio del Interior y Seguridad Pública
- Descripción: Regula la Política Nacional de Ciberseguridad.
- Contenido: Establece las directrices para la implementación de medidas de ciberseguridad en el sector público y privado.
- Objetivo: Fortalecer la capacidad de respuesta y prevención ante amenazas cibernéticas.

Reglamento N° 58 del Ministerio de Hacienda sobre Protección de Datos Personales en el Sector Público
- Descripción: Establece directrices específicas para el tratamiento de datos personales por parte de organismos públicos.
- Contenido: Define las responsabilidades de los organismos públicos en cuanto a la protección y tratamiento de datos personales.
- Objetivo: Asegurar el correcto manejo de datos personales por parte de las entidades públicas.

Proyecto de Ley de Protección de Datos Personales (Ley N° 21.096)
- Descripción: Aún en discusión en el Congreso, busca actualizar y reforzar la normativa vigente en materia de protección de datos personales.
- Contenido: Propone la creación de una Agencia de Protección de Datos Personales y establece nuevas obligaciones y derechos en materia de datos personales.
- Objetivo: Adecuar la normativa chilena a los estándares internacionales de protección de dato