Política de Seguridad de la Información - Departamento de IT

1. Introducción y Propósito

1.1 Objetivo

Esta política establece los lineamientos, procedimientos y controles necesarios para proteger la información y los sistemas de información del departamento de IT, asegurando la confidencialidad, integridad y disponibilidad de los datos.

1.2 Alcance

Esta política aplica a:

- Todo el personal del departamento de IT
- Sistemas de información y tecnología
- Datos y información procesada, almacenada o transmitida
- Contratistas y proveedores con acceso a sistemas internos

1.3 Responsabilidades

- **Director de IT**: Aprobación y supervisión de la política
- **Administradores de sistemas**: Implementación técnica de controles
- **Todo el personal**: Cumplimiento de los procedimientos establecidos

2. Clasificación de la Información

2.1 Niveles de Clasificación

- **CONFIDENCIAL**: Información crítica que podría causar daño grave si se compromete
- **INTERNO**: Información para uso interno de la organización
- **PÚBLICO**: Información que puede ser divulgada sin restricciones

2.2 Manejo por Clasificación

- Confidencial: Cifrado obligatorio, acceso restringido
- Interno: Protección estándar, acceso controlado
- Público: Sin restricciones especiales

3. Control de Acceso

3.1 Autenticación

- **Contraseñas**: Mínimo 12 caracteres, mayúsculas, minúsculas, números y símbolos
- **Autenticación multifactor (MFA)**: Obligatoria para sistemas críticos
- **Renovación**: Cambio de contraseñas cada 90 días

3.2 Autorización

- Principio de menor privilegio
- Revisión trimestral de permisos
- Desactivación inmediata de cuentas al término de contratos

3.3 Cuentas de Usuario

- Cuentas personales únicas
- Prohibición de cuentas compartidas
- Bloqueo automático tras 3 intentos fallidos

4. Seguridad en Redes

4.1 Perímetro de Red

- Firewall configurado con reglas restrictivas
- Segmentación de redes por función
- Monitoreo continuo del tráfico

4.2 Acceso Remoto

- VPN obligatoria para acceso externo
- Cifrado de todas las conexiones remotas
- Registro de todas las sesiones remotas

4.3 WiFi Corporativo

- Cifrado WPA3 mínimo
- Cambio regular de credenciales
- Red separada para invitados

5. Protección de Datos

5.1 Cifrado

- **En reposo**: AES-256 para datos sensibles
- **En tránsito**: TLS 1.3 para comunicaciones
- **Llaves**: Gestión centralizada de llaves de cifrado

5.2 Respaldos

- Respaldo diario automatizado
- Pruebas mensuales de restauración
- Almacenamiento en ubicación segura externa

5.3 Eliminación Segura

- Borrado seguro de dispositivos de almacenamiento
- Certificación de destrucción de medios

- Registro de eliminación de datos

6. Seguridad en Desarrollo

6.1 Desarrollo Seguro

- Revisiones de código obligatorias
- Pruebas de seguridad automatizadas
- Análisis de vulnerabilidades

6.2 Entornos de Desarrollo

- Separación de entornos (desarrollo, pruebas, producción)
- Datos de prueba anonimizados
- Acceso controlado a cada entorno

7. Gestión de Incidentes

7.1 Detección

- Monitoreo 24/7 de sistemas críticos
- Alertas automatizadas de seguridad
- Análisis de logs centralizado

7.2 Respuesta

- Equipo de respuesta a incidentes designado
- Procedimientos escalados por severidad
- Documentación de todos los incidentes

7.3 Recuperación

- Planes de continuidad del negocio
- Procedimientos de recuperación ante desastres
- Pruebas regulares de planes de contingencia

8. Cumplimiento y Auditoría

8.1 Auditorías

- Auditorías internas trimestrales
- Auditorías externas anuales
- Revisión continua de controles

8.2 Documentación

- Registro de cambios en sistemas
- Documentación de procedimientos
- Evidencia de cumplimiento normativo

9. Capacitación y Concientización

9.1 Programa de Capacitación

- Capacitación inicial obligatoria
- Actualización anual de conocimientos
- Simulacros de phishing trimestrales

9.2 Comunicación

- Boletines mensuales de seguridad
- Alertas de amenazas emergentes
- Canal de reporte de incidentes

10. Gestión de Proveedores

10.1 Evaluación de Proveedores

- Evaluación de seguridad antes de contratación
- Contratos con cláusulas de seguridad
- Monitoreo continuo del cumplimiento

10.2 Acceso de Terceros

- Acceso limitado y monitoreado
- Acuerdos de confidencialidad obligatorios
- Revocación inmediata al finalizar contrato

11. Dispositivos Móviles y BYOD

11.1 Dispositivos Corporativos

- Configuración de seguridad estándar
- Cifrado de dispositivos obligatorio
- Gestión centralizada (MDM)

11.2 Dispositivos Personales

- Política BYOD con restricciones
- Aplicaciones de seguridad obligatorias
- Separación de datos personales y corporativos

12. Sanciones y Violaciones

12.1 Violaciones

- Reporte inmediato de violaciones
- Investigación formal de incidentes
- Medidas correctivas documentadas

12.2 Sanciones

- Capacitación adicional

- Suspensión de privilegios
- Medidas disciplinarias según gravedad

13. Revisión y Actualización

13.1 Revisión Periódica

- Revisión anual de la política
- Actualización según amenazas emergentes
- Aprobación formal de cambios

13.2 Comunicación de Cambios

- Notificación a todo el personal
- Capacitación sobre nuevos procedimientos
- Actualización de documentación

14. Contactos de Emergencia

14.1 Equipo de Seguridad

- **Coordinador de Seguridad**: [Nombre y contacto]
- **Administrador de Sistemas**: [Nombre y contacto]
- **Responsable de Cumplimiento**: [Nombre y contacto]

14.2 Escalamiento

- Incidentes críticos: Notificación inmediata
- Incidentes menores: Reporte en 24 horas
- Canal de emergencia: [Número/email]

Fecha de Aprobación: [Fecha] **Próxima Revisión**: [Fecha + 1 año] **Versión**: 1.0 **Aprobado por**: [Director de IT]

Esta política debe ser leída, entendida y firmada por todo el personal del departamento de IT.