MANUAL DE SEGURIDAD DE LA INFORMACIÓN TV AZTECA

Dirección de Tecnología y Ciberseguridad
Políticas y Procedimientos de Seguridad 2025

MARCO DE SEGURIDAD CORPORATIVA

MISIÓN DE CIBERSEGURIDAD:
Proteger los activos digitales, la información confidencial y la continuidad operativa de TV Azteca mediante la implementación de controles de seguridad de clase mundial y una cultura de concientización en ciberseguridad.

OBJETIVOS ESTRATÉGICOS:
- Protección de información sensible 24/7
- Continuidad de operaciones de transmisión
- Cumplimiento regulatorio 100%
- Defensa contra amenazas avanzadas
- Cultura de seguridad organizacional
- Recuperación rápida ante incidentes

CLASIFICACIÓN DE LA INFORMACIÓN

INFORMACIÓN PÚBLICA:
- Programación y horarios
- Información corporativa general
- Comunicados de prensa
- Contenido transmitido
- Políticas públicas

INFORMACIÓN INTERNA:
- Estrategias de negocio
- Análisis de competencia
- Proyecciones financieras
- Planes de programación
- Documentos operativos

INFORMACIÓN CONFIDENCIAL:
- Contratos con talentos
- Datos financieros detallados
- Estrategias de contenido
- Información de empleados

- Negociaciones comerciales

INFORMACIÓN RESTRINGIDA:
- Datos personales de audiencia
- Secretos comerciales
- Tecnología propietaria
- Información legal privilegiada
- Códigos de acceso y credenciales

ARQUITECTURA DE SEGURIDAD

DEFENSA EN PROFUNDIDAD:
Capa 1 - Perímetro de Red:
- Firewalls de nueva generación (Fortinet)
- Sistemas de prevención de intrusiones
- Gateways de correo electrónico seguros
- Filtrado de contenido web
- DDoS protection

Capa 2 - Seguridad de Red Interna:
- Microsegmentación de red
- Network Access Control (NAC)
- Wireless security (WPA3)
- VPN de acceso remoto
- Zero Trust Network Access

Capa 3 - Seguridad de Endpoints:
- Antivirus de nueva generación
- EDR (Endpoint Detection Response)
- Mobile Device Management
- Patch management automatizado
- Application control

Capa 4 - Seguridad de Aplicaciones:
- Web Application Firewalls
- Secure code development
- Penetration testing
- Vulnerability scanning
- API security gateway

Capa 5 - Seguridad de Datos:
- Encriptación en reposo (AES-256)
- Encriptación en tránsito (TLS 1.3)

- Data Loss Prevention (DLP)
- Database security monitoring
- Backup encryption

INFRAESTRUCTURA DE SEGURIDAD

CENTRO DE OPERACIONES DE SEGURIDAD (SOC):
- Operación 24/7/365
- Analistas especializados: 12 personas
- SIEM enterprise: IBM QRadar
- Threat intelligence feeds: 15 fuentes
- Tiempo promedio de detección: 8 minutos
- Tiempo promedio de respuesta: 15 minutos

HERRAMIENTAS DE MONITOREO:
- Security Information Event Management (SIEM)
- User Entity Behavior Analytics (UEBA)
- Network Traffic Analysis (NTA)
- Vulnerability Management Platform
- Threat Intelligence Platform

PLATAFORMA TECNOLÓGICA:
- Forcepoint DLP Suite
- CrowdStrike Falcon EDR
- Microsoft Defender for Office 365
- Splunk Enterprise Security
- Rapid7 InsightVM

INDICADORES DE SEGURIDAD:
- Eventos de seguridad procesados: 2.3M diarios
- Alertas de alta prioridad: 45 promedio diarias
- False positive rate: <5%
- Mean Time to Detect (MTTD): 8 minutos
- Mean Time to Respond (MTTR): 15 minutos

GESTIÓN DE IDENTIDADES Y ACCESOS

DIRECTORIO ACTIVO EMPRESARIAL:
- Usuarios activos: 4,850
- Grupos de seguridad: 1,234
- Políticas de grupo: 156
- Controladores de dominio: 8

- Sincronización cloud: Azure AD

AUTENTICACIÓN MULTIFACTOR:
- Cobertura: 100% usuarios privilegiados
- Métodos: SMS, app móvil, tokens hardware
- Plataforma: Microsoft Authenticator
- Bypass temporal: Proceso autorizado
- Compliance rate: 98.5%

GESTIÓN DE ACCESOS PRIVILEGIADOS:
- Accounts privilegiadas: 345
- Password vaulting: CyberArk PAM
- Session recording: 100% sesiones admin
- Just-in-time access: Implementado
- Regular access reviews: Trimestrales

POLÍTICAS DE CONTRASEÑAS:
- Longitud mínima: 12 caracteres
- Complejidad: Letras, números, símbolos
- Rotación: 90 días para privilegiados
- Historia: 12 contraseñas anteriores
- Diccionario: Palabras comunes bloqueadas

PROTECCIÓN CONTRA AMENAZAS

AMENAZAS IDENTIFICADAS:
1. Ransomware: Prioridad crítica
2. Phishing dirigido: Alta incidencia
3. Insider threats: Monitoreo continuo
4. APT (Advanced Persistent Threats): Seguimiento
5. DDoS attacks: Defensa automática

CONTROLES ANTI-MALWARE:
- Detección basada en signatures
- Análisis comportamental
- Machine learning detection
- Sandboxing automático
- Cloud threat intelligence

EMAIL SECURITY:
- Gateway de seguridad: Proofpoint
- Anti-phishing: ATP (Advanced Threat Protection)
- DMARC, SPF, DKIM: Implementados

- Email encryption: Disponible
- User awareness: Training mensual

WEB SECURITY:
- Secure web gateway: Zscaler
- URL filtering: 98.5% cobertura
- SSL inspection: Tráfico HTTPS
- Cloud security: CASB integration
- Shadow IT discovery: Continuo

BACKUP Y CONTINUIDAD

ESTRATEGIA DE RESPALDOS:
- Backup diario: Datos críticos
- Backup semanal: Sistemas completos
- Retention: 7 años mínimo
- Testing: Mensual
- Offsite storage: 3 ubicaciones

DISASTER RECOVERY:
- RTO (Recovery Time Objective): 4 horas
- RPO (Recovery Point Objective): 1 hora
- Site secundario: Santa Fe
- Site terciario: Guadalajara
- Cloud backup: AWS S3 Glacier

BUSINESS CONTINUITY:
- Plan de continuidad: Actualizado anualmente
- Tests de DR: Trimestrales
- Comunicaciones de crisis: Definidas
- Personal de emergencia: 24/7
- Proveedores alternativos: Identificados

MÉTRICAS DE DISPONIBILIDAD:
- Uptime objetivo: 99.9%
- Uptime actual: 99.94%
- Planned downtime: <8 horas anuales
- Unplanned downtime: <4 horas anuales
- MTBF (Mean Time Between Failures): 8,760 horas

CUMPLIMIENTO REGULATORIO

MARCOS NORMATIVOS:
- Ley Federal de Protección de Datos (LFPDPPP)
- Ley General de Transparencia
- Lineamientos de Ciberseguridad CNBV
- ISO 27001: Implementación en proceso
- SOX Compliance: Sección 404

PROTECCIÓN DE DATOS PERSONALES:
- Privacy Impact Assessments: 23 realizados
- Data mapping: 100% sistemas críticos
- Consent management: Implementado
- Right to be forgotten: Proceso definido
- Data minimization: Política activa

AUDITORÍAS Y CERTIFICACIONES:
- Auditoría externa anual: KPMG
- Penetration testing: Semestral
- Vulnerability assessments: Mensual
- ISO 27001: Certificación en proceso
- SOC 2 Type II: Planeado 2025

CONTROLES FINANCIEROS:
- Segregation of duties: Implementada
- Change management: Proceso formal
- Access controls: Revisión trimestral
- System documentation: Actualizada
- Backup testing: Mensual

CONCIENTIZACIÓN EN SEGURIDAD

PROGRAMA DE CAPACITACIÓN:
- Training obligatorio: 100% empleados
- Frecuencia: Anual + actualizaciones
- Modalidad: E-learning + presencial
- Evaluación: Test online
- Certificación: Interno

SIMULACROS DE PHISHING:
- Frecuencia: Mensual
- Click rate objetivo: <5%
- Click rate actual: 3.2%
- Reporting rate: 78%
- Training automático: Usuarios vulnerables

COMUNICACIONES DE SEGURIDAD:
- Newsletter mensual: 4,850 empleados
- Alertas de seguridad: Tiempo real
- Security champions: 45 personas
- Awareness events: 6 anuales
- Posters y material: Actualizado trimestral

MÉTRICAS DE CONCIENTIZACIÓN:
- Training completion: 98.5%
- Knowledge retention: 87%
- Incident reporting: +34% vs 2024
- Security culture index: 8.2/10
- Employee satisfaction: 89%

GESTIÓN DE INCIDENTES

CLASIFICACIÓN DE INCIDENTES:
Nivel 1 - Crítico:
- Interrupción de transmisión
- Breach de datos masivo
- Ransomware activo
- Compromiso de sistemas críticos

Nivel 2 - Alto:
- Malware detectado
- Phishing exitoso
- Fuga de datos menor
- Indisponibilidad de sistemas

Nivel 3 - Medio:
- Violación de políticas
- Intentos de acceso no autorizado
- Vulnerabilidades críticas
- Anomalías en el comportamiento

Nivel 4 - Bajo:
- Vulnerabilidades menores
- Falsos positivos
- Incidentes informativos
- Requests de soporte

PROCESO DE RESPUESTA:

1. Detección y alerta (0-5 min)
2. Análisis inicial (5-15 min)
3. Containment (15-30 min)
4. Eradication (30 min - 4 hrs)
5. Recovery (4-24 hrs)
6. Lessons learned (1 semana)

EQUIPO DE RESPUESTA (CSIRT):
- CISO: Líder del equipo
- Security analysts: 4 personas
- IT operations: 2 personas
- Legal counsel: 1 persona
- Communications: 1 persona
- External experts: Según necesidad

COMUNICACIÓN DE INCIDENTES:
- Internal stakeholders: Inmediato
- Executive team: 1 hora
- Board notification: 24 horas
- Regulatory bodies: Según ley
- Public disclosure: Según impacto

MÉTRICAS DE INCIDENTES 2024:
- Total incidentes: 1,234
- Críticos: 4 (0.3%)
- Altos: 23 (1.9%)
- Medios: 156 (12.6%)
- Bajos: 1,051 (85.2%)
- MTTC (Mean Time to Contain): 45 min

SEGURIDAD EN LA NUBE

CLOUD SECURITY FRAMEWORK:
- Shared responsibility model: Implementado
- Cloud security posture: Automatizado
- Container security: Implementado
- Serverless security: Monitoreo
- Multi-cloud strategy: AWS + Azure

CONTROLES ESPECÍFICOS:
- Identity federation: Single sign-on
- Network security groups: Microsegmentación
- Data encryption: Keys management

- Logging and monitoring: 100% cobertura
- Compliance automation: CSPM tools

PROVEEDORES CLOUD:
- Amazon Web Services: Primary
- Microsoft Azure: Secondary
- Google Cloud Platform: Específico
- Security certifications: Verificadas
- Data residency: México prioritario

CONFIGURACIONES SEGURAS:
- CIS Benchmarks: Implementados
- Security baselines: Automatizadas
- Vulnerability scanning: Continuo
- Patch management: Automatizado
- Change control: Proceso formal

TECNOLOGÍAS EMERGENTES

INTELIGENCIA ARTIFICIAL:
- AI for threat detection: Implementando
- Machine learning: Security analytics
- Behavioral analysis: User activity
- Automated response: Nivel 1 incidents
- False positive reduction: 40% mejora

ZERO TRUST ARCHITECTURE:
- Never trust, always verify: Principio
- Micro-segmentation: Implementando
- Identity-centric security: Adoptando
- Least privilege access: Implementado
- Continuous verification: Desarrollando

BLOCKCHAIN SECURITY:
- Smart contracts: Security review
- Cryptocurrency: Policy defined
- Distributed ledger: Pilot projects
- Digital identity: Research phase
- Supply chain: Potential application

QUANTUM CRYPTOGRAPHY:
- Post-quantum algorithms: Monitoring
- Key distribution: Research

- Migration planning: Future state
- Vendor assessment: Ongoing
- Standards monitoring: NIST guidelines

MÉTRICAS Y REPORTES

INDICADORES CLAVE DE RENDIMIENTO:
- Security events per day: 2.3M
- High priority alerts: 45/day
- False positive rate: <5%
- Vulnerability patch time: 72 hrs critical
- User training completion: 98.5%

REPORTES DE GESTIÓN:
- Daily security briefing: CISO
- Weekly incident summary: IT management
- Monthly security dashboard: Executive team
- Quarterly risk assessment: Board
- Annual security report: Stakeholders

MÉTRICAS FINANCIERAS:
- Security budget: $45M pesos anuales
- Cost per employee: $9,278 pesos
- ROI security investment: 4.2x
- Avoided losses: $123M pesos estimados
- Insurance premium reduction: 15%

BENCHMARKING INDUSTRIA:
- Security maturity: Top 25% industry
- Incident response time: Better than average
- Training effectiveness: Industry leading
- Investment level: Above average
- Compliance score: 98.5%

PROYECTOS FUTUROS 2025

INVERSIÓN PLANIFICADA: $67M pesos

INICIATIVAS CLAVE:
- Zero Trust implementation: $23M
- AI security platform: $18M
- Cloud security enhancement: $12M

- Quantum-ready cryptography: $8M
- Security automation: $6M

CRONOGRAMA EJECUCIÓN:
Q2 2025: Zero Trust fase 1
Q3 2025: AI platform deployment
Q4 2025: Cloud security upgrade
Q1 2026: Quantum crypto pilot
Q2 2026: Automation rollout

RESULTADOS ESPERADOS:
- 50% reducción incidentes
- 75% faster incident response
- 90% automation routine tasks
- 99.99% uptime critical systems
- ISO 27001 certification

CONTACTO SEGURIDAD

Centro de Operaciones de Seguridad: 55-1720-1313 ext. 7777
Email: security@tvazteca.com
Incidentes de seguridad: incident.response@tvazteca.com
CISO: Ing. Roberto Alcántara Pérez
Security Manager: Lic. Ana Patricia Morales
Reportes de vulnerabilidades: vulnerability@tvazteca.com