NTP ISO/27001:2014: Tecnologías de la Información, Técnicas de Seguridad, Sistema de Gestión de Seguridad de la Información (DOMINIOS)

- **A5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**
  - A5.1 Dirección de la Gerencia para la Seguridad de la Información
    - A5.1.1 Políticas para la Seguridad de la Información
    - A5.1.2 Revisión de las Políticas para la Seguridad de la Información
- **A6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
  - A6.1 Organización Interna
    - A6.1.1 Roles y responsabilidades en Seguridad de la Información
    - A6.1.2 Segregación de funciones
    - A6.1.3 Contacto con autoridades
    - A6.1.4 Contacto con grupos especiales de interés
    - A6.1.5 Seguridad de la Información en la Gestión de Proyectos
  - A6.2 Dispositivos móviles y teletrabajo
    - A6.2.1 Política de dispositivos móviles
    - A6.2.2 Teletrabajo
- **A7 SEGURIDAD DE LOS RECURSOS HUMANOS**
  - A7.1 Antes del empleo
    - A7.1.1 Selección
    - A7.1.2 Términos y condiciones del empleo
  - A7.2 Durante el empleo
    - A7.2.1 Responsabilidades de la Gerencia
    - A7.2.2 Concienciación, educación y capacitación en seguridad de la información
    - A7.2.3 Proceso disciplinario
  - A7.3 Terminación y cambio de empleo
    - A7.3.1 Terminación o cambio de responsabilidades del empleo
- **A8 GESTIÓN DE ACTIVOS**
  - A8.1 Responsabilidad por los activos
    - A8.1.1 Inventario de activos
    - A8.1.2 Propiedad de los activos
    - A8.1.3 Uso aceptable de los activos
    - A8.1.4 Retorno de activos
  - A8.2 Clasificación de la información
    - A8.2.1 Clasificación de la Información
    - A8.1.2 Etiquetado de la información
    - A8.1.3 Manejo de activos
  - A8.3 Manejo de medios
    - A8.3.1 Gestión de los medios removibles
    - A8.3.2 Disposición de medios
    - A8.3.3 Transferencia de medios físicos
- **A9 CONTROL DE ACCESO**
  - A9.1 Requisitos de la empresa para el control de acceso
    - A9.1.1 Política de control de acceso
    - A9.1.2 Acceso a las redes y servicios de red
  - A9.2 Gestión de acceso de usuario
    - A9.2.1 Registro y baja de usuario
    - A9.2.2 Aprovisionamiento de acceso a usuario
    - A9.2.3 Gestión de derechos de acceso privilegiado
    - A9.2.4 Gestión de información de autenticación secreta de usuarios
    - A9.2.5 Revisión de los derechos de acceso de usuario
    - A9.2.6 Remoción o ajuste de derechos de acceso
  - A9.3 Responsabilidades de los usuarios
    - A9.3.1 Uso de información de autenticación secreta
  - A9.4 Control de acceso a sistemas y aplicaciones
    - A9.4.1 Restricción de acceso a la información
    - A9.4.2 Procedimientos de ingreso seguro
    - A9.4.3 Sistema de gestión de contraseñas
    - A9.4.4 Uso de programas utilitarios privilegiados
    - A9.4.5 Control de acceso al código fuente de los programas
- **A10 CRIPTOGRAFÍA**
  - A10.1 Controles criptográficos
    - A10.1.1 Políticas para la Seguridad de la Información
    - A10.1.2 Gestión de claves
- **A11 SEGURIDAD FÍSICA Y AMBIENTAL**
  - A11.1 Áreas seguras
    - A11.1.1 Perímetro de seguridad física
    - A11.1.2 Controles de ingreso físico
    - A11.1.3 Asegurar oficinas, áreas e instalaciones
    - A11.1.4 Protección contra las amenazas externas y ambientales
    - A11.1.5 Trabajo en áreas seguras
    - A11.1.6 Áreas de despacho y carga
  - A11.2 Seguridad de los equipos
    - A11.2.1 Emplazamiento y protección de los equipos
    - A11.2.2 Servicios de suministro
    - A11.2.3 Seguridad del cableado
    - A11.2.4 Mantenimiento de equipos
    - A11.2.5 Remoción de activos
    - A11.2.6 Seguridad de equipos y activos fuera de las instalaciones
    - A11.2.7 Disposición o reutilización segura de equipos
    - A11.2.8 Equipos de usuario desatendidos
    - A11.2.9 Política de escritorio limpio y pantalla limpia
- **A12 SEGURIDAD DE LAS OPERACIONES**
  - A12.1 Procedimientos y responsabilidades operativas
    - A12.1.1 Procedimientos operativos documentados
    - A12.1.2 Gestión del cambio
    - A12.1.3 Gestión de la capacidad
    - A12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones.
  - A12.2 Protección contra códigos maliciosos
    - A12.2.1 Controles contra códigos maliciosos
  - A12.3 Respaldo
    - A12.3.1 Respaldo de la información
  - A12.4 Registros y monitoreo
    - A12.4.1 Registro de eventos
    - A12.4.2 Protección de información de registros
    - A12.4.3 Registros del administrador y del operador
    - A12.4.4 Sincronización del reloj
  - A12.5 Control del software en explotación
    - A12.5.1 Instalación de software en sistems operacionales
  - A12.6 Gestión de la vulnerabilidad técnica
    - A12.6.1 Gestión de vulnerabilidades técnicas
    - A12.6.2 Restricciones sobre la instalación de software
  - A12.7 Consideraciones para la auditoría de los sistemas de información
    - A12.7.1 Controles de auditoría de sistemas de información
- **A13 SEGURIDAD DE LAS COMUNICACIONES**
  - A13.1 Gestión de seguridad de la red
    - A13.1.1 Controles de la red
    - A13.1.2 Seguridad de servicios de red
    - A13.1.3 Segregación en redes
  - A13.2 Transferencia de información
    - A13.2.1 Políticas y procedimientos de transferencia de la información
    - A13.2.2 Acuerdo sobre transferencia de información
    - A13.2.3 Mensajes electrónicos
    - A13.2.4 Acuerdos de confidencialidad o no divulgación
- **A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
  - A14.1 Requisitos de seguridad de los sistemas de información
    - A14.1.1 Análisis y especificación de requisitos de seguridad de la información
    - A14.1.2 Aseguramiento de servicios de aplicaciones sobre redes públicas
    - A14.1.3 Protección de transacciones en servicios de aplicación
  - A14.2 Seguridad en los procesos de desarrollo y soporte
    - A14.2.1 Política de desarrollo seguro
    - A14.2.2 Procedimientos de control de cambio del sistema
    - A14.2.3 Revisión técnica de aplicaciones despúes de cambios a la plataforma operativa
    - A14.2.4 Restricciones sobre cambios a los paquetes de software
    - A14.2.5 Principios de ingeniería de sistemas seguros
    - A14.2.6 Ambiente de desarrollo seguro
    - A14.2.7 Desarrollo contratado externamente
    - A14.2.8 Pruebas de seguridad del sistema
    - A14.2.9 Pruebas de aceptación del sistema
  - A14.3 Datos de prueba
    - A14.3.1 Protección de datos de prueba
- **A15 RELACIONES CON LOS PROVEEDORES**
  - A15.1 Seguridad de la información en las relaciones con los proveedores
    - A15.1.1 Política de seguridad de la información para las relaciones con los proveedores
    - A15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores
    - A15.1.3 Cadena de suministro de tecnología de información y comunicación
  - A15.2 Gestión de entrega de servicio del proveedor
    - A15.2.1 Monitoreo y revisión de servicios de los proveedores
    - A15.2.2 Gestión de cambios a los servicios de proveedores
- **A16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
  - A16.1 Gestión de incidentes de seguridad de la información
    - A16.1.1 Responsabilidades y procedimientos
    - A16.1.2 Reporte de eventos de sesguridad de la información
    - A16.1.3 Reporte de debilidades de seguridad de la información
    - A16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información
    - A16.1.5 Respuesta a incidentes de seguridad de la información
    - A16.1.6 Aprendizaje de los incidentes de seguridad de la información
    - A16.1.7 Recopilación de evidencias
- **A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**
  - A17.1 Continuidad de seguridad de la información
    - A17.1.1 Planificación de continuidad de seguridad de la información
    - A17.1.2 Implementación de continuidad de seguridad de la información
    - A17.1.3 Verificación, revisión y evaluación de continuidad de seguridad de la información
  - A17.2 Redundancia
    - A17.2.1 Instalaciones de procesamiento de la información
- **A18 CUMPLIMIENTO**
  - A18.1 Cumplimiento con requisitos legales y contractuales
    - A18.1.1 Identificación de requisitos contractuales y de legislación aplicables
    - A18.1.2 Derechos de Propiedad Intelectual
    - A18.1.3 Protección de registros
    - A18.1.4 Privacidad y protección de datos personales
    - A18.1.5 Regulación de controles criptográficos
  - A18.2 Revisiones de seguridad de la información
    - A18.2.1 Revisión independiente de la seguridad de la información
    - A18.2.2 Cumplimiento de políticas y normas de seguridad
    - A18.2.3 Revisión del cumplimiento técnico