UNIVERSIDAD CENTRAL DEL ECUADOR

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CARRERA DE SISTEMAS DE INFORMACIÓN

SEGURIDAD Y GESTIÓN DE RIESGO EN LAS TI

ESTUDIANTE

Heredia Nicolalde
Vanessa Nayeli

TEMA

ANEXO A ISO/IEC 27001:2013.

DOCENTE

CHRISTIAN PATRICIO ESPINOSA MARIN

FECHA

23/12/2025

Estructura del Anexo A (ISO/IEC 27001:2013)

La nueva versión agrupa los controles en 114 medidas de seguridad clasificadas en 14 categorías o dominios principales.

N° de Cláusula	**Categoría del Control**	**Cantidad de Controles**	**Objetivo Principal**
A.5	Políticas de Seguridad	2	Proporcionar dirección y soporte a la seguridad de la información.
A.6	Organización de la Seguridad	7	Establecer un marco de gestión para la implementación de la seguridad.
A.7	Seguridad de RR.HH.	6	Asegurar que los empleados y contratistas entiendan sus responsabilidades.
A.8	Gestión de Activos	10	Identificar activos y definir responsabilidades de protección.
A.9	Control de Acceso	14	Limitar el acceso a la información y recursos de procesamiento.
A.10	Criptografía	2	Asegurar el uso adecuado y eficaz del cifrado para proteger los datos.
A.11	Seguridad Física y Ambiental	15	Prevenir accesos físicos no autorizados y daños a las instalaciones.
A.12	Seguridad de Operaciones	14	Asegurar la operación correcta y segura de las instalaciones de TI.
A.13	Seguridad de Comunicaciones	7	Proteger la información en las redes y su infraestructura de soporte.
A.14	Adquisición y Mantenimiento	13	Garantizar que la seguridad sea parte integral de los sistemas de información.
A.15	Relación con Proveedores	5	Asegurar la protección de activos accesibles por proveedores externos.
A.16	Gestión de Incidentes	7	Asegurar un enfoque consistente para gestionar eventos de seguridad.
A.17	Continuidad del Negocio	4	Proteger la seguridad de la información durante interrupciones.
A.18	Cumplimiento	8	Evitar el incumplimiento de obligaciones legales y contractuales.
TOTAL		**114**	

A.5 Políticas de Seguridad de la Información

N∘	Control
A.5.1.1	Políticas para la seguridad de la información
A.5.1.2	Revisión de las políticas para la seguridad de la información

A.6 Organización de la Seguridad de la Información

N∘	Control
A.6.1.1	Roles y responsabilidades para la seguridad de la información2
A.6.1.23	Segregación de tareas4
A.6.1.35	Contacto con las autoridades6
A.6.1.47	Contacto con grupos de interés especial8
A.6.1.59	Seguridad de la información en la g10estión de proyectos
A.6.2.1	Política de dispositivos móviles
A.6.2.2	Teletrabajo

A.7 Seguridad de los Recursos Humanos

N∘	Control
A.7.1.1	Selección (Investigación de antecedentes)
A.7.1.2	Términos y condiciones del empleo
A.7.2.1	Responsabilidades de la dirección
A.7.2.2	Concientización, educación y capacitación en seguridad
A.7.2.3	Proceso disciplinario
A.7.3.1	Terminación o cambio de responsabilidades de empleo

A.8 Gestión de Activos

N∘	Control
A.8.1.11112	Inventario de activos1314
A.8.1.21516	Propiedad de los activos1718
A.8.1.31920	Uso aceptable de los activos2122
A.8.1.42324	Devolución de activos2526
A.8.2.12728	Clasificación de la información2930
A.8.2.23132	Etiquetado de la información3334
A.8.2.33536	Manej37o de activos38
A.8.3.139	Gestión de medios removibl40es
A.8.3.2	Eliminación de medios
A.8.3.3	Transferencia de medios físicos

A.9 Control de Acceso

N∘	Control
A.9.1.1	Política de control de acceso
A.9.1.2	Acceso a las redes y servicios de red
A.9.2.1	Registro y baja de usuarios
A.9.2.2	Provisión de acceso de usuario
A.9.2.3	Gestión de derechos de acceso privilegiado
A.9.2.4	Gestión de información de autenticación secreta de usuarios

A.9.2.5	Revisión de los derechos de acceso de usuario
A.9.2.6	Retiro o adaptación de los derechos de acceso
A.9.3.1	Uso de información de autenticación secreta
A.9.4.1	Restricción del acceso a la información
A.9.4.2	Procedimientos de acceso seguro
A.9.4.3	Sistema de gestión de contraseñas
A.9.4.4	Uso de programas de utilidad con privilegios
A.9.4.5	Control de acceso al código fuente de los programas

A.10 Criptografía

No	Control
A.10.1.1	Política sobre el uso de controles criptográficos
A.10.1.2	Gestión de llaves

A.11 Seguridad Física y Ambiental

No	Control	No	Control
A.11.1.1	Perímetro de seguridad física	A.11.2.1	Emplazamiento y protección de equipos
A.11.1.2	Controles físicos de entrada	A.11.2.2	Servicios de apoyo (energía, agua)
A.11.1.3	Seguridad de oficinas y salas	A.11.2.3	Seguridad del cableado
A.11.1.4	Protección contra amenazas externas	A.11.2.4	Mantenimiento de equipos
A.11.1.5	Trabajo en áreas seguras	A.11.2.5	Retiro de activos
A.11.1.6	Áreas de carga y descarga	A.11.2.6	Seguridad de equipos fuera de sitio
A.11.2.7	Eliminación segura de equipos	A.11.2.9	Política de escritorio y pantalla limpia

A.12 Seguridad de las Operaciones

No	Control	No	Control
A.12.1.1	Procedimientos de operación	A.12.4.1	Registro de eventos
A.12.1.2	Gestión de cambios	A.12.4.2	Protección de la información de registro
A.12.1.3	Gestión de la capacidad	A.12.4.3	Registros del administrador y operador
A.12.1.4	Separación de entornos	A.12.4.4	Sincronización del reloj
A.12.2.1	Controles contra el malware	A.12.5.1	Instalación de software en sistemas
A.12.3.1	Respaldo de información	A.12.6.1	Gestión de vulnerabilidades técnicas
A.12.6.2	Restricción de instalación de software	A.12.7.1	Controles de auditoría de sistemas

A.13 Seguridad de las Comunicaciones

Nº	Control
A.13.1.1	Controles de red
A.13.1.2	Seguridad de los servicios de red
A.13.1.3	Segregación de redes
A.13.2.1	Políticas y procedimientos de transferencia
A.13.2.2	Acuerdos sobre transferencia de información
A.13.2.3	Mensajería electrónica
A.13.2.4	Acuerdos de confidencialidad o no divulgación

A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas

Nº	Control	Nº	Control
A.14.1.1	Análisis de requisitos de seguridad	A.14.2.4	Restricciones a cambios en software
A.14.1.2	Seguridad en redes públicas	A.14.2.5	Principios de ingeniería de sistemas
A.14.1.3	Seguridad en transacciones de servicios	A.14.2.6	Entorno de desarrollo seguro
A.14.2.1	Política de desarrollo seguro	A.14.2.7	Desarrollo tercerizado
A.14.2.2	Procedimientos de control de cambios	A.14.2.8	Pruebas de seguridad del sistema
A.14.2.3	Revisión técnica de aplicaciones	A.14.3.1	Protección de datos de prueba

A.15 Relaciones con los Proveedores

Nº	Control
A.15.1.1	Política de seguridad para proveedores
A.15.1.2	Seguridad en acuerdos con proveedores
A.15.1.3	Cadena de suministro de TIC
A.15.2.1	Seguimiento y revisión de servicios de proveedores
A.15.2.2	Gestión de cambios en servicios de proveedores

A.16 Gestión de Incidentes de Seguridad

Nº	Control
A.16.1.1	Responsabilidades y procedimientos
A.16.1.2	Reporte de eventos de seguridad
A.16.1.3	Reporte de debilidades de seguridad
A.16.1.4	Evaluación y decisión sobre eventos
A.16.1.5	Respuesta a incidentes de seguridad
A.16.1.6	Aprendizaje de los incidentes
A.16.1.7	Recolección de evidencia

A.17 Aspectos de Seguridad para la Continuidad del Negocio

No	Control
A.17.1.1	Planificación de la continuidad de seguridad
A.17.1.2	Implementación de la continuidad de seguridad
A.17.1.3	Verificación y evaluación de la continuidad
A.17.2.1	Disponibilidad de medios de procesamiento

A.18 Cumplimiento

No	Control
A.18.1.1	Identificación de la legislación aplicable
A.18.1.2	Derechos de propiedad intelectual
A.18.1.3	Protección de registros
A.18.1.4	Privacidad y protección de datos personales
A.18.1.5	Regulación de controles criptográficos
A.18.2.1	Revisión independiente de la seguridad
A.18.2.2	Cumplimiento con las políticas de seguridad
A.18.2.3	Revisión de cumplimiento técnico