ANEXO A.1 REFERENCIA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN - ISO 27001:2022

5. Controles organizacionales	6. Controles de personas	8. Controles Tecnológicos
5.1. Políticas de Seguridad de la Información	6.1. Chequeo	8.1. Dispositivos de punto final de usuario
5.2. Roles y responsabilidades de seguridad de la información	6.2. Términos y condiciones de empleo	8.2. Derechos de acceso privilegiado
5.3. Separación de funciones	6.3. Concientización, educación y capacitación en seguridad de la información	8.3. Restricción de acceso a la información
5.4. Responsabilidades de Gestión	6.4. Proceso Disciplinario	8.4. Acceso al código fuente
5.5. Contacto con las autoridades	6.5. Responsabilidades después de la terminación o cambio de empleo	8.5. Autenticación segura
5.6. Contacto con grupos de interés especial	6.6. Acuerdos de confidencialidad o no divulgación	8.6. Gestión de capacidad
5.7. Inteligencia de Amenazas	6.7. Trabajo remoto	8.7. Protección contra malware
5.8. Seguridad de la información en la gestión de proyectos.	6.8. Informes de eventos de seguridad de la información	8.8. Gestión de vulnerabilidades técnicas
5.9. Inventario de información y otros activos asociados	**7. Controles Físicos**	8.9. Gestión de la configuración
5.10. Uso aceptable de la información y otros activos asociados	7.1. Perímetro de seguridad física	8.10. Eliminación de información
5.11. Devolución de activos	7.2. Entrada física	8.11. Enmascaramiento de datos
5.12. Clasificación de la información	7.3. Asegurar oficinas, salas e instalaciones	8.12. Prevención de fuga de datos
5.13. Etiquetado de información	7.4. Monitoreo de seguridad física	8.13. Copia de seguridad de la información
5.14. Transferencia de información	7.5. Protección contra amenazas físicas y ambientales.	8.14. Redundancia de las instalaciones de procesamiento de información
5.15. Control de acceso	7.6. Trabajar en áreas seguras	8.15. Inicio sesión
5.16. Gestión de identidad	7.7. Escritorio despejado y pantalla despejada	8.16. Actividades de seguimiento
5.17. Información de autenticación	7.8. Emplazamiento y protección de equipos	8.17. Sincronización de reloj
5.18. Derechos de acceso	7.9. Seguridad de los activos fuera de las instalaciones	8.18. Uso de programas de utilidad privilegiados
5.19. Seguridad de la información en las relaciones con los proveedores	7.10. Medios de almacenamiento	8.19. Instalación de software en sistemas operativos
5.20. Abordar la seguridad de la información en los acuerdos con los proveedores	7.11. Utilidades de apoyo	8.20. Seguridad de la red
5.21. Gestión de la seguridad de la información en la cadena de suministro de las TIC	7.12. Seguridad del cableado	8.21. Seguridad de los servicios de red.
5.22. Seguimiento, revisión y gestión de cambios de servicios de proveedores	7.13. Mantenimiento de equipos	8.22. Segregación de redes
5.23. Seguridad de la información para el uso de servicios en la nube	7.14. Eliminación segura o reutilización de equipos	8.23. Filtrado web
5.24. Planificación y preparación de la gestión de incidentes de seguridad de la información		8.24. Uso de criptografía
5.25. Evaluación y decisión sobre eventos de seguridad de la información		8.25. Ciclo de vida de desarrollo seguro
5.26. Respuesta a incidentes de seguridad de la información		8.26. Requisitos de seguridad de la aplicación
5.27. Aprender de los incidentes de seguridad de la información		8.27. Principios de arquitectura e ingeniería de sistemas seguros
5.28. Recolección de evidencia		8.28. Codificación segura
5.29. Seguridad de la información durante la interrupción		8.29. Pruebas de seguridad en desarrollo y aceptación
5.30. Preparación de las TIC para la continuidad del negocio		8.30. Desarrollo subcontratado
5.31. Requisitos legales, estatutarios, reglamentarios y contractuales		8.31. Separación de los entornos de desarrollo, prueba y producción
5.32. Derechos de propiedad intelectual		8.32. Gestión del cambio
5.33. Protección de registros		8.33. Información de la prueba
5.34. Privacidad y protección de la información identificable de la persona (PII)		8.34. Protección de los sistemas de información durante las pruebas de auditoría
5.35. Revisión independiente de la seguridad de la información.		
5.36. Cumplimiento de políticas, normas y estándares de seguridad de la información		
5.37. Procedimientos operativos documentados		

*Nuevos controles 2022