CATALOGO DE CONTROLES RUC

A.5 – Medidas Organizativas (Organizational Controls) (37 controles)

Nº	Control	Proceso interno	Cobertura RUC
5.1	Políticas de seguridad de la información	Redacción, aprobación y difusión	Plantilla editable + seguimiento de revisiones
5.2	Revisión de políticas	Revisión anual o por cambios críticos	Alertas automáticas de revisión
5.3	Roles y responsabilidades	Asignación de funciones y dueños de activos	Gestión de roles en plataforma
5.4	Separación de funciones	Segregación de funciones críticas	Registro de permisos y revisiones
5.5	Responsabilidad de la dirección	Compromiso y apoyo al SGSI	Dashboard de KPIs para dirección
5.6	Coordinación de seguridad	Comité de seguridad	Gestión de reuniones y acuerdos
5.7	Contacto con autoridades	Procedimiento de comunicación oficial	Registro y seguimiento de contactos
5.8	Contacto con grupos de interés	Comunicación con CERTs, sector, etc.	Agenda de contactos relevantes
5.9	Revisión independiente	Auditorías externas	Registro de auditorías y hallazgos
5.10	Revisión por la dirección	Evaluación periódica del SGSI	Módulo de informes ejecutivos
5.11	Seguridad en relaciones con proveedores	Evaluación y contratos	Gestión documental con cláusulas de seguridad
5.12	Seguridad en la cadena de suministro	Evaluación de terceros	Checklist de cumplimiento de proveedores
5.13	Aceptación de uso de activos	Políticas de uso aceptable	Firma electrónica de políticas
5.14	Retiro de activos	Baja controlada de equipos	Registro de bajas y destrucción
5.15	Seguridad de la información para teletrabajo	Procedimiento de trabajo remoto seguro	Política editable + checklist

5.16	Seguridad en dispositivos móviles	Controles para BYOD o corporativos	Inventario y seguimiento
5.17	Clasificación de la información	Etiquetado y niveles de acceso	Campos personalizables en inventario
5.18	Etiquetado de la información	Procedimiento de etiquetado físico/digital	Campo de clasificación integrado
5.19	Manejo de soportes removibles	Procedimiento de uso seguro	Registro de entrega y destrucción
5.20	Eliminación segura de la información	Procedimiento de borrado seguro	Registro con evidencia
5.21	Transferencia de información	Procedimiento seguro (cifrado, SFTP)	Registro de envíos críticos
5.22	Acuerdos de confidencialidad	NDAs y cláusulas contractuales	Gestión de documentos y vencimientos
5.23	Protección de registros	Controles de acceso y respaldo	Repositorio seguro en RUC
5.24	Privacidad y protección de datos personales	Cumplimiento de normativas (GDPR, etc.)	Políticas y registros de consentimiento
5.25	Cumplimiento legal	Lista de leyes aplicables	Módulo de requisitos legales
5.26	Gestión de propiedad intelectual	Registro y protección	Repositorio con control de acceso
5.27	Uso aceptable de activos	Procedimiento y capacitación	Política editable + firma digital
5.28	Procedimiento disciplinario	Sanciones por incumplimientos	Registro de incidentes disciplinarios
5.29	Identificación de riesgos	Metodología documentada	Matriz de riesgos automatizada
5.30	Evaluación de riesgos	Evaluación periódica	Flujo guiado en RUC
5.31	Tratamiento de riesgos	Plan de acción	Gestión de tareas y responsables
5.32	Aprobación de tratamiento	Validación por dirección	Flujos de aprobación en plataforma
5.33	Seguimiento de tratamiento	Control de avances	Dashboard de estado

5.34	Plan de continuidad	Desarrollo y pruebas	Plantilla editable + checklists
5.35	Pruebas de continuidad	Ejecución de simulacros	Registro y resultados
5.36	Revisión de continuidad	Ajuste de plan	Alertas de revisión
5.37	Mejora continua del SGSI	Aplicar lecciones aprendidas	Registro de mejoras

A.6 – Medidas de Personas (People Controls) (8 controles)

Nº	Control	Proceso interno	Cobertura RUC
6.1	Verificación previa a contratación	Background check	Registro de verificación
6.2	Términos y condiciones laborales	Inclusión de cláusulas de seguridad	Gestión documental
6.3	Concientización y capacitación	Plan de formación	Registro y seguimiento de capacitaciones
6.4	Disciplina en seguridad	Aplicación de sanciones	Registro de incidentes
6.5	Responsabilidades durante el empleo	Cumplimiento de políticas	Firma digital
6.6	Cambio o terminación de empleo	Baja controlada de accesos	Checklist de offboarding
6.7	Responsabilidad post-terminación	Acuerdos de no divulgación	Gestión de vencimientos
6.8	Protección contra amenazas internas	Monitoreo y protocolos	Registro de incidentes

A.7 – Medidas Físicas (Physical Controls) (14 controles)

Nº	Control	Proceso interno	Cobertura RUC
7.1	Perímetro de seguridad física	Controles de acceso físico	Registro de autorizaciones
7.2	Zonas seguras	Áreas restringidas	Mapa y lista de accesos
7.3	Controles de entrada	Tarjetas, biometría	Registro de entradas
7.4	Protección contra amenazas ambientales	Sensores, climatización	Registro de mantenimiento
7.5	Seguridad en oficinas y salas	Control de acceso físico	Listado de accesos
7.6	Trabajos en áreas seguras	Procedimientos autorizados	Registro de autorizaciones
7.7	Protección de equipos	Anclajes, UPS	Inventario con ubicación
7.8	Eliminación segura de equipos	Procedimiento documentado	Registro con evidencia
7.9	Reubicación segura de equipos	Checklist de traslado	Registro de movimiento
7.10	Seguridad en zonas públicas	Control visual	Registro de rondas
7.11	Protección contra desastres	Sistemas antiincendio	Registro de inspecciones
7.12	Entrada de mantenimiento	Control de proveedores externos	Registro de accesos
7.13	Seguridad en cables y redes	Protección física	Checklist de inspección
7.14	Supervisión física	Cámaras y rondas	Registro de revisión

A.8 – Medidas Tecnológicas (Technological Controls) (34 controles)

Nº	Control	Proceso interno	Cobertura RUC
8.1	Gestión de identidades	Creación, modificación, baja	Registro y aprobaciones
8.2	Autenticación de usuarios	MFA, contraseñas seguras	Registro de configuración
8.3	Autorización de accesos	Principio de mínimo privilegio	Flujos de aprobación
8.4	Revisión de accesos	Auditorías periódicas	Alertas y reportes
8.5	Eliminación de accesos	Offboarding seguro	Registro con evidencia
8.6	Gestión de privilegios	Control de cuentas admin	Registro de cambios
8.7	Protección contra malware	Antivirus, EDR	Registro de actualizaciones
8.8	Copias de seguridad	Procedimientos y pruebas	Registro de backups y restores
8.9	Seguridad en redes	Firewalls, segmentación	Registro de cambios
8.10	Cifrado de datos	En tránsito y en reposo	Registro de configuración
8.11	Monitoreo de sistemas	SIEM, alertas	Registro de eventos
8.12	Gestión de vulnerabilidades	Escaneo y remediación	Registro de parches
8.13	Seguridad en aplicaciones	Pruebas de seguridad	Registro de revisiones
8.14	Desarrollo seguro	Ciclo de vida seguro (SDLC)	Registro de controles
8.15	Protección en entornos de prueba	Datos anonimizados	Registro de autorizaciones
8.16	Gestión de cambios	Procedimiento formal	Registro y aprobación
8.17	Monitoreo de capacidad	Uso de CPU, RAM, red	Dashboard
8.18	Respuesta a incidentes	Protocolo de actuación	Registro y análisis
8.19	Registro de eventos	Logs centralizados	Integración SIEM
8.20	Análisis de logs	Detección de anomalías	Reportes
8.21	Sincronización horaria	NTP	Registro de configuración

8.22	Seguridad de software	Listado de aplicaciones autorizadas	Inventario
8.23	Control de puertos y protocolos	Restricciones de uso	Registro de configuración
8.24	Seguridad en IoT	Configuración segura	Registro de dispositivos
8.25	Seguridad en la nube	Configuración y monitoreo	Checklist de revisión
8.26	Gestión de certificados	Emisión y renovación	Alertas de vencimiento
8.27	Prevención de pérdida de datos (DLP)	Herramientas DLP	Registro de incidentes
8.28	Revisión de seguridad	Auditorías técnicas	Registro de hallazgos
8.29	Integridad de software	Hash, firmas digitales	Registro
8.30	Eliminación segura de datos	Procedimiento de borrado	Registro
8.31	Seguridad en redes inalámbricas	WPA3, autenticación	Registro
8.32	Seguridad de endpoints	Configuración de hardening	Checklist
8.33	Seguridad de correo	Anti-phishing, SPF/DKIM	Registro
8.34	Respaldo de sistemas críticos	Plan de recuperación	Registro