

RESULTADO PLAN DE IMPLEMENTACIÓN — NTC-ISO 9001:2015 + ISO/IEC 27001:2022 Berruit S.A.S.							
CLÁUSULAS 4 AL 10 — ESTRUCTURA DE ALTO NIVEL ARMONIZADA (HLS)							
Cláusula / Capítulo	Norma	Requisito	Cumple (C)	Cumple Parcialmente (CP)	No Cumple (NC)	No Aplica (NA)	Evidencia Documental
CAPÍTULO 4 — CONTEXTO DE LA ORGANIZACIÓN							
4.1	ISO 9001:2015 + ISO 27001:2022	Comprensión de la organización y de su contexto La organización debe determinar las cuestiones externas e internas pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión.	X				P-DE-01 Procedimiento Dirección Estratégica (análisis PESTAL, DOFA, DODA/FOFA). Dirección Estratégica Berruit.(D-DE-01 a D-DE-15) MT-SGI-02 Matriz de Riesgos del SIG (contexto gerencial y de gestión integral) SOA-SGI-01.
4.2	ISO 9001:2015 + ISO 27001:2022	Comprensión de las necesidades y expectativas de las partes interesadas La organización debe determinar las partes interesadas pertinentes al sistema de gestión, sus requisitos y cuáles de estos requisitos son aplicables.	X				P-DE-01 (identificación de partes interesadas). SISTEMA DE GESTIÓN INTEGRADO - Política y Objetivos Integrados.xlsx. MT-SGI-01 Matriz de Comunicación
4.3	ISO 9001:2015 + ISO 27001:2022	Determinación del alcance del sistema de gestión La organización debe determinar los límites y la aplicabilidad del sistema de gestión para establecer su alcance, considerando cuestiones externas/interinas, requisitos de partes interesadas, y productos y servicios.	X				Política del SGI SOA-SGI-01 Declaración de Aplicabilidad (define alcance SGSI: outsourcing IT, ciberseguridad, administración de infraestructura, respaldo y continuidad). F-SGI-06 Caracterización de Proceso SGI.
4.4	ISO 9001:2015 + ISO 27001:2022	Sistema de gestión y sus procesos La organización debe establecer, implementar, mantener y mejorar continuamente el sistema de gestión, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta Norma.	X				F-SGI-06 Caracterización de Procesos (todos los procesos). MAPA DE PROCESOS 2025 L-SGI-01 Listado Maestro de Registros. F-SGI-07 Ficha Técnica de Indicadores por proceso.
NIVEL DE CUMPLIMIENTO — CAPÍTULO 4			4	0	0	0	100,0%
CAPÍTULO 5 — LIDERAZGO							
5.1	ISO 9001:2015 + ISO 27001:2022	Liderazgo y compromiso La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión: estableciendo política y objetivos compatibles con la dirección estratégica, asegurando la integración del SGI en los procesos de negocio, y promoviendo la mejora continua.		X			Política del SGI (Revisada por Alta Dirección). PO-SGE-01 Política de Seguridad de la información y Ciberseguridad (declaración de Alta Dirección). F-SGI-08 Planificación y Gestión de Objetivos. F-SGI-07 Fichas de Indicadores.
5.1.2	ISO 9001:2015	Enfoque al cliente La alta dirección debe demostrar liderazgo asegurando que: los requisitos del cliente y los requisitos de partes interesadas, y determinar los riesgos que afectan la conformidad se tratan; y se mantiene el enfoque en el aumento de la satisfacción del cliente.	X				F-CL-01 Acuerdo de Nivel de Servicio (ANS-SLA). F-SGE-07 Encuesta de Satisfacción al Cliente. P-CL-01 Procedimiento Comercial. P-SGI-03 Procedimiento PQRSF. F-SGI-02 Registro de PQRSF.
5.2	ISO 9001:2015 + ISO 27001:2022	Política del sistema de gestión La alta dirección debe establecer, implementar y mantener una política que sea apropiada al propósito y contexto de la organización; proporcione un marco para los objetivos, incluya compromisos de cumplimiento de requisitos aplicables y de mejora continua; esté disponible como información documentada y sea comunicada.	X				Política del SGI de Berruit. (vigente). PO-SGE-01 Política de SI (vigente). política del SGI para la web.pdf (comunicada externamente). MT-SGI-01 Matriz de Comunicación.
5.3	ISO 9001:2015 + ISO 27001:2022	Roles, responsabilidades y autoridades en la organización La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen, se comuniquen y se entiendan en la organización.	X				OR-RH-01 Organigrama. MRH-01 a MRH-08 Manuales de Funciones y Perfil. SOA-SGI-01 (responsables por control del Anexo A). Carta de designación formal del rol Responsable del SGSI/CISO con delegación de autoridad expresa por parte de la Alta Dirección.
NIVEL DE CUMPLIMIENTO — CAPÍTULO 5			3	1	0	0	87,5%
CAPÍTULO 6 — PLANIFICACIÓN							
6.1	ISO 9001:2015 + ISO 27001:2022	Acciones para abordar riesgos y oportunidades — General Al planificar el sistema de gestión, la organización debe considerar el contexto y los requisitos de partes interesadas, y determinar los riesgos y oportunidades que deben abordarse para asegurar que el SGI logre sus resultados previstos, prevenga efectos no deseados y logre la mejora continua.	X				MT-SGI-02 Matriz de Riesgos del SIG (Matriz Gerencial y Gestión Integral). P-DE-01 PROCEDIMIENTO DIRECCIÓN ESTRATEGICA F-SGI-08 Planificación y Gestión de Objetivos.
6.1.2	ISO 27001:2022	Evaluación de riesgos de seguridad de la información La organización debe definir y aplicar un proceso de evaluación de riesgos de SI que: establezca criterios de aceptación de riesgo; identifique, analice y evalúe los riesgos de SI; y conserve información documentada sobre los resultados.	X				MT-SGI-02 Matriz de Riesgos del SIG (incluye riesgos de SI). SOA-SGI-01 (columna "Riesgos" relacionado(s)). F-SGE-12 Registro de Vulnerabilidades y Plan de Remediación.
6.1.3	ISO 27001:2022	Tratamiento de riesgos de seguridad de la información La organización debe definir y aplicar un proceso de tratamiento de riesgos que seleccione opciones de tratamiento, determine controles necesarios, compare con el Anexo A, produzca una Declaración de Aplicabilidad (SoA) y un Plan de Tratamiento de Riesgos (PTR).	X				SOA-SGI-01 Declaración de Aplicabilidad (93 controles, con justificación, estado y evidencia). MT-SGI-02 Matriz de Riesgos (planes de tratamiento). Procedimientos P-SGE-7 (controles implementados).
6.2	ISO 9001:2015 + ISO 27001:2022	Objetivos del sistema de gestión y planificación para lograrlos La organización debe establecer objetivos del SGI coherentes con la política, medibles, con seguimiento, comunicados y actualizados. Debe determinar qué se hará, qué recursos se requerirán, quién será responsable, cuándo se completará y cómo se evaluarán los resultados.	X				SISTEMA DE GESTIÓN INTEGRADO - Política y Objetivos Integrados. F-SGI-07 Fichas Técnicas de Indicadores por proceso. F-SGI-08 Planificación y Gestión de Objetivos.
6.3	ISO 9001:2015	Planificación de los cambios Cuando la organización determine la necesidad de cambios en el SGC, los cambios deben llevarse a cabo de manera planificada, considerando el propósito, las consecuencias potenciales, la integridad del sistema, la disponibilidad de recursos y la reasignación de responsabilidades.	X				P-SGE-06 Procedimiento Gestión de Cambios en el Entorno de TI. F-SGE-04 Formato RFC.
NIVEL DE CUMPLIMIENTO — CAPÍTULO 6			5	0	0	0	100,0%
CAPÍTULO 7 — SOPORTE							
7.1	ISO 9001:2015 + ISO 27001:2022	Recursos La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión, considerando capacidades internas y necesidades de proveedores externos.	X				F-DE-01 Presupuesto Anual. P-DE-01 Procedimiento Dirección Estratégica (asignación de recursos). MRH-01 a MRH-08 (recursos humanos). F-SGE-11 Inventario de Activos TI (recursos tecnológicos).
7.2	ISO 9001:2015 + ISO 27001:2022	Competencia La organización debe determinar la competencia necesaria, asegurarse de que las personas sean competentes (educación, formación, experiencia), tomar acciones cuando sea necesario y conservar información documentada como evidencia de la competencia.	X				F-RH-01 Formato de Proceso de Selección. MRH-01 a MRH-08 Manuales de Funciones (competencias requeridas). P-RH-01 Procedimiento Selección. P-RH-02 Procedimiento Capacitación. CR-RH-01 Cronograma de Capacitación. L-RH-01 Lista de Asistencia.
7.3	ISO 9001:2015 + ISO 27001:2022	Toma de conciencia Las personas bajo el control de la organización deben tomar conciencia de: la política del sistema de gestión; los objetivos pertinentes, su contribución a la eficacia del SGI; y las implicaciones del incumplimiento de los requisitos.	X				Onboarding Analista IT .pdf. Onboarding Auxiliar Mesa de Ayuda.pdf. Onboarding Coordinador Soporte IT .pdf. Onboarding Ejecutivos B2B.pdf. Onboarding Analista de Prospección Evaluación de Inducción F-RH-02 Acuerdo de Confidencialidad. CR-RH-01 Cronograma de Capacitación. Certificados en fabricantes (Soporte IT, Ejecutivos B2B)
7.4	ISO 9001:2015 + ISO 27001:2022	Comunicación La organización debe determinar las comunicaciones internas y externas pertinentes al sistema de gestión: qué comunicar, cuándo comunicarlo, a quién comunicarlo, cómo comunicarlo y quién lo comunica.	X				MT-SGI-01 Matriz de Comunicación V1 (qué, cuándo, a quién, cómo, responsable). política del SGI para la web.pdf (comunicación externa).
7.5	ISO 9001:2015 + ISO 27001:2022	Información documentada — General / Creación / Control El sistema de gestión de la organización debe incluir la información documentada requerida por la norma y la determinada como necesaria para la eficacia del SGI. La organización debe controlar la creación, actualización y distribución de la información documentada.	X				L-SGI-01 Listado Maestro de Registros. F-SGI-06 Caracterizaciones de Proceso. P-SGE-27 Clasificación y RBAC. Microsoft 365/SharePoint como plataforma de gestión documental. Todos los documentos con código, versión y fecha estandarizados.
NIVEL DE CUMPLIMIENTO — CAPÍTULO 7			5	0	0	0	100,0%
CAPÍTULO 8 — OPERACIÓN							
8.1	ISO 9001:2015 + ISO 27001:2022	Planificación y control operacional La organización debe planificar, implementar, controlar, revisar y mantener los procesos necesarios para cumplir los requisitos de prestación de productos y servicios, e implementar las acciones determinadas para abordar riesgos y oportunidades.	X				F-SGI-06 Caracterizaciones de Proceso (criterios operacionales por proceso). P-SGE-01 Procedimiento de Soporte IT. P-CL-01 Procedimiento Comercial. P-CM-01 Procedimiento de Compras. F-SGE-08 Monitoreo Alertas. F-SGE-10 Informe Mensual Monitoreo. SOA-SGI-01 (controles implementados).
8.2	ISO 9001:2015	Requisitos para los productos y servicios La organización debe establecer procesos de comunicación con los clientes, determinar los requisitos del servicio (incluyendo legales/reglamentarios) y revisarlos antes de comprometerse con el cliente.	X				F-CL-01 ANS-SLA. P-CL-01 Procedimiento Comercial. Modelo de Propuesta de Servicios.docx. Modelo de Propuesta Comercial de Productos.docx. F-SGE-07 Encuesta de Satisfacción. Portal de Productos y Servicios.pdf.

8.4	ISO 9001:2015 + ISO 27001:2022	Control de los procesos, productos y servicios suministrados externamente La organización debe asegurarse de que los procesos, productos y servicios suministrados externamente sean conformes a los requisitos. Debe determinar los controles a aplicar y comunicar a los proveedores sus requisitos.	X				P-CM-01 Procedimiento Compras. F-CM-01 Selección y Evaluación de Proveedor (100 puntos, 8 criterios). F-CM-04 Reevaluación de Proveedor. F-CM-05 Confidencialidad de Proveedores y Terceros. F-CM-06 Verificación de Calidad. F-CM-02 Acta de Entrega. F-CM-03 Orden de Compra.	
8.7	ISO 9001:2015 + ISO 27001:2022	Control de las salidas no conformes La organización debe asegurarse de que las salidas que no sean conformes con los requisitos se identifiquen, controlen y traten para prevenir su uso o entrega no intencionados. Las acciones deben ser apropiadas a la naturaleza y efectos de la no conformidad.	X				P-SGI-04 Procedimiento Control SNC, NC y AC. F-SGI-03 Registro de Salidas No Conformes. F-SGI-04 Autorización RMA TI. F-SGI-05 Registro de Devolución Cerrada. P-SGI-05 Procedimiento Devolución de Productos.	
NIVEL DE CUMPLIMIENTO — CAPÍTULO 8			4	0	0	0	100,0%	
CAPÍTULO 9 — EVALUACIÓN DEL DESEMPEÑO								
9.1	ISO 9001:2015 + ISO 27001:2022	Seguimiento, medición, análisis y evaluación La organización debe determinar qué necesita seguimiento y medición; los métodos aplicables; cuándo se llevan a cabo y cuándo se analizan los resultados. Para ISO 27001, debe incluir la evaluación del desempeño y la eficacia del SGSI.	X				F-SGI-07 Fichas Técnicas de Indicadores (todos los procesos: SGI, Dirección Estratégica, Comercial, Soporte IT Externo, Compras, RRRHH, Soporte IT Interno). F-STE-09 Registro Monitoreo Alertas. F-SGI-10 Informe Mensual Monitoreo. MT-SGI-06 Plan Auditoría Seguridad Técnica Anual (En revisión)	
9.1.2	ISO 9001:2015	Satisfacción del cliente La organización debe realizar el seguimiento de las percepciones del cliente sobre el grado en que se cumplen sus necesidades y expectativas. Debe determinar los métodos para obtener, realizar el seguimiento y revisar esta información.	X				F-SGI-02 Registro de PQRSF. P-SGI-03 Procedimiento PQRSF. F-CL-01 ANS-SLA (métricas de cumplimiento).	Implementar un índice consolidado CSAT/NPS con metodología estandarizada, frecuencia trimestral y análisis de tendencias como insumo para la revisión por la dirección
9.2	ISO 9001:2015 + ISO 27001:2022	Auditoría interna La organización debe llevar a cabo auditorías internas a intervalos planificados para determinar si el sistema de gestión es conforme con los requisitos propios y los de la norma, y si se implementa y mantiene eficazmente.		X			MT-SGI-06 Plan de Auditoría de Seguridad Técnica Anual. P-DE-01 (referencia a auditorías). L-SGI-01 Listado Maestro.	Desarrollar un Programa Anual de Auditoría Interna del SGI Integrado que cubra todos los procesos y requisitos de ambas normas, con registro de hallazgos y seguimiento de acciones correctivas.
9.3	ISO 9001:2015 + ISO 27001:2022	Revisión por la dirección La alta dirección debe revisar el SGI a intervalos planificados para asegurar su conveniencia, adecuación, eficacia y alineación estratégica. La revisión debe incluir entradas específicas y producir salidas documentadas (decisiones y acciones).		X			P-DE-01 Procedimiento Dirección Estratégica (incluye ciclo de revisión estratégica). F-SGI-07 Fichas Indicadores (insumos). SISTEMA DE GESTIÓN INTEGRADO - Política y Objetivos.	Implementar un formato de Acta de Revisión por la Dirección que cubra todas las entradas requeridas por ambas normas, con registro de decisiones, responsables y fechas de seguimiento.
NIVEL DE CUMPLIMIENTO — CAPÍTULO 9			0	2	2	0	25,0%	
CAPÍTULO 10 — MEJORA								
10.1	ISO 9001:2015 + ISO 27001:2022	Mejora — General La organización debe determinar y seleccionar las oportunidades de mejora e implementar cualquier acción necesaria para cumplir los requisitos y aumentar la satisfacción del cliente / mejorar continuamente la conveniencia, adecuación y eficacia del SGI.	X				P-SGI-04 Procedimiento NC y AC (mejora reactiva). F-SGI-15 Registro de Lecciones Aprendidas. P-SGI-48 Procedimiento Lecciones Aprendidas de Incidentes de SI.	Implementar un mecanismo de gestión de oportunidades de mejora proactivas con priorización, asignación, seguimiento y cierre formal, alimentado por múltiples fuentes (auditorías, indicadores, benchmarking, sugerencias del equipo).
10.2	ISO 9001:2015 + ISO 27001:2022	No conformidad y acción correctiva Cuando ocurra una no conformidad, la organización debe: reaccionar, evaluar la necesidad de acciones para eliminar las causas, implementar las acciones correctivas, revisar su eficacia, actualizar riesgos y oportunidades si es necesario, y hacer cambios al SGI si fuera preciso.	X				P-SGI-04 Procedimiento Control SNC, NC y AC (ciclo completo: identificación, registro, causa raíz, corrección, AC, seguimiento y cierre). F-SGI-03 Registro de Salidas No Conformes.	Asegurar que F-SGI-03 registre la verificación de eficacia con fecha, responsable y criterio utilizado. Incluir análisis de tendencias de NC en la revisión por la dirección.
10.3	ISO 27001:2022	Mejora continua La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de seguridad de la información.		X			P-SGI-48 Lecciones Aprendidas de Incidentes de SI. F-SGI-15 Registro de Lecciones Aprendidas. P-SGI-45 Auditorías Técnicas y Pentesting (en revisión). MT-SGI-06 Plan Auditoría Seguridad Técnica (en revisión)	Formalizar el ciclo de mejora continua del SGSI mediante un informe anual de estado que consolide: resultados de auditorías, incidentes, métricas de controles, avance del SOA y decisiones de mejora.
NIVEL DE CUMPLIMIENTO — CAPÍTULO 10			1	2	0	0	66,7%	

CUADRO RESUMEN DE CUMPLIMIENTO DEL SGI INTEGRADO — ISO 9001:2015 + ISO/IEC 27001:2022

Capítulo	Nombre	Cumple (C)	Cumple Perc. (CP)	No Cumple (NC)	No Aplica (NA)	% Cumplimen to
Capítulo 4	Contexto	4	0	0	0	100,0%
Capítulo 5	Liderazgo	3	1	0	0	87,5%
Capítulo 6	Planificación	5	0	0	0	100,0%
Capítulo 7	Soporte	5	0	0	0	100,0%
Capítulo 8	Operación	4	0	0	0	100,0%
Capítulo 9	Desempeño	0	2	2	0	25,0%
Capítulo 10	Mejora	1	2	0	0	66,7%

RESULTADO PLAN DE IMPLEMENTACIÓN — ANEXO A ISO/IEC 27001:2022 Berruit S.A.S.							
93 CONTROLES DE SEGURIDAD — CATEGORÍAS: ORGANIZACIONAL • PERSONAS • FÍSICO • TECNOLÓGICO							
Control	Nombre del Control	Categoría	Cumple (C)	Cumple Parcialmente (CP)	No Cumple (NC)	No Aplica (NA)	Evidencia Documental
RECOMENDACIONES							
CONTROLES ORGANIZACIONALES (A.5.1 – A.5.37)							
A.5.1	Políticas para la seguridad de la información	Organizacional	X				PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. Política del SGI para la web D-DE-06 Política y Objetivos SGI
A.5.2	Roles y responsabilidades de seguridad de la información	Organizacional	X				M-RH-01 a M-RH-08 Manuales de Funciones. OR-RH-01 Organigrama. SOA-SGI-01 (responsables por control).
A.5.3	Segregación de funciones	Organizacional	X				M-RH-01 a M-RH-08 Manuales de funciones G-STE-01 Guía Privilegio Mínimo por Rol. MT-STE-02 Matriz de Permisos por Rol y Plataforma.
A.5.4	Responsabilidades de la dirección	Organizacional		X			PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. F-SGI-07 Indicadores SGI. D-DE-06 Política y Objetivos SGI F-SGI-08 Planificación y Gestión de Objetivos
A.5.5	Contacto con autoridades	Organizacional	X				D-DE-08 PESTAL (referencia normativa a SIC, COLCERT, MINTIC, DIAN) MT-STE-07 DIRECTORIO FORMAL DE CONTACTOS REGULATORIOS Y DE RESPUESTA A INCIDENTES P-STE-46 PROCEDIMIENTO DE PROTOCOLO DE NOTIFICACIÓN DE INCIDENTES A ENTES REGULADORES
A.5.6	Contacto con grupos de interés especial	Organizacional		X			MT-STE-08 Registro de Suscripciones a Grupos Especializados y Fuentes de Inteligencia.
A.5.7	Inteligencia de amenazas	Organizacional	X				D-DE-08 PESTAL. F-STE-12 Registro de Vulnerabilidades P-STE-30 Gestión de Vulnerabilidades P-STE-47 PROCEDIMIENTO DE PARTICIPACIÓN EN COMUNIDADES DE CIBERSEGURIDAD Y GESTIÓN DE INTELIGENCIA DE AMENAZAS MT-STE-08 REGISTRO DE SUSCRIPCIONES – GRUPOS ESPECIALIZADOS E INTELIGENCIA DE AMENAZAS
A.5.8	Seguridad de la información en gestión de proyectos	Organizacional		X			P-STE-16 Desarrollo y Gestión de Proyectos de TI. G-STE-09 Caracterización de Proceso. G-STE-07 Principios de Arquitectura Segura P-STE-06 Gestión de Cambios en el Entorno de TI
A.5.9	Inventario de información y otros activos	Organizacional	X				F-STE-11 Inventario de Activos y Plataformas TI. P-STE-11 Procedimiento Control de Inventario de Activos IT L-STE-01 Listado de Rutas Backups
A.5.10	Uso aceptable de la información y activos	Organizacional	X				PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. F-RH-02 Acuerdo de Confidencialidad. P-STE-13 Política de Uso Aceptable de Recursos TI.
A.5.11	Devolución de activos	Organizacional	X				P-STE-32 Eliminación y Disposición Segura de Activos F-STE-13 Registro de Eliminación y Disposición Segura P-STE-02 Control de Acceso (proceso de baja). F-STE-14 Checklist Formal de Desvinculación. F-RH-02 Acuerdo de Confidencialidad y Compromiso
A.5.12	Clasificación de la información	Organizacional	X				P-STE-27 Procedimiento de Clasificación de la Información y Control de Acceso (RBAC).
A.5.13	Etiquetado de la información	Organizacional		X			P-STE-27 Procedimiento de Clasificación (incluye etiquetado).
A.5.14	Transferencia de información	Organizacional		X			MT-SGI-01 Matriz de Comunicación (canales autorizados: Teams, M365, GLPI). PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. I-STE-01 Instructivo VPN FortiClient & RDP P-STE-41 Gestión Criptográfica y de Claves P-STE-02 Control de Acceso a Sistemas. F-STE-03 Solicitud de Acceso.
A.5.15	Control de acceso	Organizacional	X				F-STE-05 Solicitud de Roles y Permisos G-STE-01 Privilegio Mínimo. MT-STE-02 Permisos. Azure AD/M365
A.5.16	Gestión de identidades	Organizacional		X			P-STE-02 (ciclo de vida identidades). F-STE-03 Solicitud de Acceso. P-STE-28 Gestión de Identidades. Azure AD como IdP. F-STE-05 Solicitud de Roles y Permisos
A.5.17	Información de autenticación	Organizacional	X				P-STE-08 Gestión de Contraseñas. G-STE-01 Privilegio Mínimo. KeePass AES-256. MFA obligatorio en plataformas críticas. P-STE-26 Gestión de Accesos Privilegiados (PAM)
A.5.18	Derechos de acceso	Organizacional		X			P-STE-02 Control de Acceso. MT-STE-02 Matriz de Permisos por Rol y Plataforma P-STE-26 Gestión de Accesos Privilegiados (PAM). P-STE-28 Gestión de Identidades y Accesos
A.5.19	Seguridad en relaciones con proveedores	Organizacional	X				P-CM-01 Procedimiento de Compras F-CM-01 Selección, Evaluación Proveedor y Contratista F-CM-05 Confidencialidad de proveedores F-CM-04 Reevaluación.
A.5.20	Seguridad en contratos con proveedores	Organizacional		X			P-STE-42 Evaluación de Seguridad para Adquisición de Software G-STE-06 Checklist Requisitos de Seguridad Software Adquirido F-CM-01 Evaluación de Proveedor
A.5.21	Gestión de SI en cadena de suministro TIC	Organizacional	X				P-CM-01 Procedimiento de Compras F-CM-01 SELECCIÓN EVALUACIÓN PROVEEDOR Y CONTRATISTA F-CM-04 Reevaluación de Proveedor P-STE-42 Evaluación de Seguridad para Adquisición de Software G-STE-06 Checklist Requisitos de Seguridad Software Adquirido
A.5.22	Seguimiento y revisión de servicios de proveedores	Organizacional	X				F-CM-04 Reevaluación de Proveedor. F-CM-01 SELECCIÓN EVALUACIÓN PROVEEDOR Y CONTRATISTA F-CM-04 Reevaluación de Proveedor
A.5.23	Seguridad en servicios en la nube	Organizacional	X				P-STE-12 Gestión de Servicios en la Nube. PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. I-STE-01 Instructivo VPN FortiClient & RDP
A.5.24	Planificación de gestión de incidentes de SI	Organizacional	X				P-STE-09 Respuesta ante Incidentes. P-STE-24 Continuidad del Negocio. P-STE-20 Monitoreo y Gestión de Incidentes P-SGI-04 PROCEDIMIENTO CONTROL DE SALIDAS NO CONFORMES, NO CONFORMIDADES Y ACCIONES CORRECTIVAS GLPI (clasificación por tipo y prioridad) P-STE-09 Respuesta ante Incidentes de Seguridad en TI
A.5.25	Evaluación y decisión sobre eventos de SI	Organizacional	X				P-STE-21 Gestión de Incidentes P-STE-20 Monitoreo y Gestión de Incidentes P-STE-09 Registro Monitoreo Alertas F-CL-01 ACUERDO DE NIVEL DE SERVICIO (ANS-SLA)
A.5.26	Respuesta a incidentes de SI	Organizacional	X				P-STE-09 Respuesta ante Incidentes de Seguridad en TI P-SGI-04 PROCEDIMIENTO CONTROL DE SALIDAS NO CONFORMES, NO CONFORMIDADES Y ACCIONES CORRECTIVAS GLPI. F-CL-01 SLA
A.5.27	Aprendizaje de incidentes de SI	Organizacional	X				F-STE-15 Registro de Lecciones Aprendidas. P-STE-48 Procedimiento Lecciones Aprendidas de Incidentes de SI. P-SGI-04 Procedimiento Salidas No Conformes F-SGI-03 Salidas No Conformes

A.5.28	Recolección de evidencia	Organizacional	X				F-STE-16 Plantilla de Cadena de Custodia. P-STE-49 Preservación y Cadena de Custodia de Evidencias Digitales.	Se recomienda realizar pruebas periódicas del procedimiento de cadena de custodia con el fin de validar su aplicabilidad, eficacia y el adecuado registro de las evidencias obtenidas durante la atención de incidentes. Asimismo, es importante verificar que el personal técnico involucrado haya recibido capacitación en conceptos básicos de informática forense, garantizando que conozca los principios para la preservación, recolección, documentación y manejo adecuado de evidencias digitales, reduciendo el riesgo de comprometer su integridad o validez.
A.5.29	Si durante la interrupción	Organizacional	X				P-STE-24 Continuidad del Negocio (BIA, RTO/RPO). P-STE-14 Pruebas de Recuperación ante Desastres.	
A.5.30	Preparación TIC para continuidad del negocio	Organizacional	X				P-STE-24 Continuidad del Negocio. P-STE-03 Respaldo y Restauración de Datos P-STE-19 Gestión de Respaldo y Recuperación de Datos L-STE-01 Listado de Rutas de Backups. P-STE-14 Pruebas de Recuperación	
A.5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Organizacional	X				D-DE-08 PESTAL (Ley 1581, Ley 1273, Decreto 338, CONPES 3995) F - SGI - 09 Control Normativo D-DE-15 Partes Interesadas F-CM-05 Confidencialidad	
A.5.32	Derechos de propiedad intelectual	Organizacional	X				P-STE-17 Actualización y Gestión de Licencias de Software. P-STE-11 INVENTARIO DE ACTIVOS Y PLATAFORMAS TI P-CM-01 Procedimiento de Compras	
A.5.33	Protección de registros	Organizacional	X				L-SGI-01 LISTADO MAESTRO DE REGISTROS L-STE-01 Listado de Rutas Backups F-SGI-06 Caracterizaciones de Procesos P-STE-36 Gestión de Logs, Retención y Trazabilidad P-SGI-01 PROCEDIMIENTO PARA LA ELABORACIÓN DE DOCUMENTOS, CONTROL Y ACTUALIZACIÓN DE DOCUMENTOS DEL SGI	
A.5.34	Privacidad y protección de datos personales	Organizacional	X				F-RH-02 Acuerdo de Confidencialidad. F-CM-05 Confidencialidad de Proveedores F-RH-02 Acuerdo de Confidencialidad F-STE-08 Ficha Técnica Cliente Política de tratamiento de Datos (página web) P-STE-33 PROCEDIMIENTO DE ENMASCARAMIENTO Y ANONIMIZACIÓN DE DATOS P-STE-34 PROCEDIMIENTO DE PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) Política de tratamiento de Datos, disponible en la página web	
A.5.35	Revisión independiente de la SI	Organizacional		X			MT-STE-06 Plan de Auditoría de Seguridad Técnica Anual. P-STE-45 Auditorías Técnicas y Pruebas de Penetración.	Programar revisión independiente del SGSI (externa o de segunda parte) anualmente, adicional a las pruebas técnicas.
A.5.36	Cumplimiento de políticas, normas y estándares de SI	Organizacional		X			PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. P-SGI-04 NC y AC. MT-STE-06 Plan de Auditoría.	Se recomienda implementar autoevaluaciones periódicas de cumplimiento para cada proceso de la organización, utilizando un checklist estructurado con base en los lineamientos establecidos en el PO-STE-01 y los controles definidos en la Declaración de Aplicabilidad (SoA). Estas revisiones permitirán identificar oportunamente desviaciones, verificar la efectividad de los controles implementados, promover la mejora continua y generar evidencias objetivas del nivel de cumplimiento del Sistema de Gestión de Seguridad de la Información.
A.5.37	Procedimientos de operación de TI documentados	Organizacional	X				P-STE-01 a P-STE-49 (49 procedimientos) P-SGI-01 a P-SGI-05; P-CM-01; P-CL-01; P-RH-01 PROCEDIMIENTO PARA LA SELECCIÓN DE PERSONAL G-STE-01 a G-STE-07 (7 guías técnicas)	
NIVEL DE CUMPLIMIENTO — CATEGORÍA A.5			26	11	0	0		65,1%
CONTROLES DE PERSONAS (A.6.1 – A.6.8)								
A.6.1	Selección	Personas	X				P-RH-01 Procedimiento Selección de Personal. F-RH-01 Formato de Proceso de Selección. M-RH-01 a M-RH-08 Manuales de Funciones	
A.6.2	Términos y condiciones de empleo	Personas	X				F-RH-02 Acuerdo de Confidencialidad y Compromiso de Uso Adecuado de Activos Onboarding por rol	
A.6.3	Toma de conciencia, educación y formación en SI	Personas	X				CR-RH-01 Cronograma de Capacitación. P-RH-02 Procedimiento Capacitación. L-RH-01 Lista de Asistencia. Onboarding por rol.	
A.6.4	Proceso disciplinario	Personas	X				F-RH-02 Acuerdo de Confidencialidad (menciona consecuencias de incumplimiento). — (Reglamento Interno de Trabajo — externo al SGI)	
A.6.5	Responsabilidades tras finalización o cambio de empleo	Personas	X				F-STE-14 Checklist de Desvinculación. F-RH-02 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO DE USO ADECUADO DE LOS ACTIVOS DE INFORMACIÓN P-STE-02 Revocación de accesos.	
A.6.6	Acuerdos de confidencialidad y no divulgación	Personas	X				F-RH-02 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO DE USO ADECUADO DE LOS ACTIVOS DE INFORMACIÓN F-CM-05 Confidencialidad de Proveedores y Terceros. Contratos de los empleados Contrato de los clientes	
A.6.7	Trabajo remoto	Personas	X				P-STE-13 Política Uso Aceptable. P-STE-25 Gestión de Dispositivos Móviles y BYOD. G-STE-04 Esquema de Segmentación. I-STE-01 Instructivo VPN FortiClient & RDP	
A.6.8	Reporte de eventos de SI	Personas	X				P-STE-09 Respuesta ante Incidentes (canal de reporte). GLPI plataforma de tickets. P-STE-21 Gestión de Incidentes. P-SGI-03 Procedimiento PQRSF F-SGI-02 Registro de PQRSF MT-SGI-01 Matriz de Comunicación	
NIVEL DE CUMPLIMIENTO — CATEGORÍA A.6			8	0	0	0		100,0%
CONTROLES FÍSICOS (A.7.1 – A.7.14)								
A.7.1	Perímetros de seguridad física	Físico	X				P-STE-01 Procedimiento de Soporte IT (trabajo en sitio) G-STE-04 Esquema de Segmentación de Red. PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. Contratos con clientes	Aunque este requisito no aplica directamente para Bernul debido a la naturaleza de su operación, se recomienda desarrollar e implementar un checklist de seguridad física mínima que deba ser verificado antes de prestar servicios en las instalaciones de los clientes. Este listado puede contemplar aspectos como controles de acceso, identificación del personal autorizado, condiciones de las áreas de trabajo, restricciones de ingreso a zonas críticas y mecanismos de registro de visitas, con el fin de promover buenas prácticas de seguridad, reducir riesgos durante la prestación del servicio y evidenciar la debida diligencia de la organización frente a los entornos donde interviene.
A.7.2	Controles de entrada física	Físico	X				P-STE-02 Control de Acceso (físico y lógico). G-STE-04 Esquema de Segmentación.	Se recomienda definir e implementar controles de acceso físico para las visitas de técnicos a las instalaciones de los clientes, estableciendo requisitos mínimos como la identificación visible del personal autorizado, el acompañamiento por parte de un responsable designado cuando aplique y el registro de ingreso y salida de cada visita. Estas medidas contribuirán a fortalecer la seguridad física, garantizar la trazabilidad de las intervenciones realizadas y reducir el riesgo de accesos no autorizados a áreas o activos críticos del cliente.
A.7.3	Seguridad de oficinas, despachos e instalaciones	Físico				X	— EXCLUIDO (justificado en SoA SOA-SGI-01) Sin instalaciones físicas propias. P-STE-13 Política Uso Aceptable (seguridad de oficina remota). G-STE-02 Configuración Segura.	
A.7.4	Monitoreo de la seguridad física	Físico				X	— EXCLUIDO (justificado en SoA SOA-SGI-01) Sin instalaciones físicas propias. P-STE-09 Registro Monitoreo Alertas. P-STE-07 Monitoreo de Redes y Sistemas.	
A.7.5	Protección contra amenazas físicas y ambientales	Físico	X				P-STE-24 Continuidad del Negocio. P-STE-04 Mantenimiento Preventivo de Equipos. CR-STE-01 Cronograma de Mantenimiento	
A.7.6	Trabajo en áreas seguras	Físico	X				P-STE-13 Política Uso Aceptable. G-STE-02 Configuración Segura.	
A.7.7	Escritorio despejado y pantalla limpia	Físico	X				P-STE-13 Política de Uso Aceptable de Recursos de TI.	
A.7.8	Ubicación y protección de equipos	Físico	X				F-STE-11 Inventario de Activos y Plataformas TI P-STE-25 Gestión de Dispositivos Móviles y BYOD P-STE-04 Mantenimiento Preventivo. G-STE-02 Configuración Segura.	
A.7.9	Seguridad de los activos fuera de las instalaciones	Físico	X				P-STE-25 Gestión de Dispositivos Móviles y BYOD. P-STE-13 Procedimiento de Política Uso Aceptable. F-STE-11 Inventario de Activos y Plataformas TI	

A.7.10	Medios de almacenamiento	Físico	X				P-STE-25 Gestión de Dispositivos Móviles y BYOD P-STE-32 Eliminación y Disposición Segura de Activos F-STE-13 Registro de Eliminación.	
A.7.11	Servicios de suministro	Físico	X				P-STE-24 Continuidad del Negocio (energía, conectividad). MT-STE-05 Inventario de Servicios de Red Contratados. I-STE-01 Instructivo VPN FortiClient & RDP	
A.7.12	Seguridad del cableado	Físico				X	— EXCLUIDO (justificado en SoA, SOA-SGI-01) F-STE-06 Inventario de Cableado de Red y Voz.	
A.7.13	Mantenimiento de equipos	Físico	X				P-STE-04 Mantenimiento Preventivo de Equipos TI. CR-STE-01 Cronograma de Mantenimiento. F-STE-02 Reporte de Mantenimiento	
A.7.14	Eliminación y reutilización segura de equipos	Físico	X				P-STE-32 Eliminación y Disposición Segura de Activos F-STE-13 Registro de Eliminación y Disposición Segura	
NIVEL DE CUMPLIMIENTO — CATEGORÍA A.7			9	2	0	3	90,9%	

CONTROLES TECNOLÓGICOS (A.8.1 – A.8.34)								
A.8.1	Dispositivos de usuario final	Tecnológico	X				PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. P-STE-25 Gestión de Dispositivos Móviles y BYOD. G-STE-02 Configuración Segura. F-STE-11 Inventario de Activos.	
A.8.2	Derechos de acceso con privilegios	Tecnológico	X				P-STE-26 Gestión de Accesos Privilegiados (PAM). G-STE-01 Guía de Privilegio Mínimo por Rol MT-STE-02 Matriz de Permisos por Rol y Plataforma MT-STE-04 Inventario de Herramientas Privilegiadas.	
A.8.3	Restricción de acceso a la información	Tecnológico	X				P-STE-02 Control de Acceso a Sistemas P-STE-27 Clasificación y RBAC. MT-STE-02 Matriz de Permisos por Rol y Plataforma.	
A.8.4	Acceso al código fuente	Tecnológico				X	— EXCLUIDO (justificado en SoA SOA-SGI-01) P-STE-44 Separación de Ambientes. P-STE-15 Desarrollo y Gestión de Proyectos.	
A.8.5	Autenticación segura	Tecnológico	X				P-STE-02 Control de Acceso a Sistemas P-STE-08 Gestión de Contraseñas P-STE-28 Gestión de Identidades y Accesos	
A.8.6	Gestión de la capacidad	Tecnológico	X				P-STE-23 Procedimiento de Gestión de la Capacidad. P-STE-07 Monitoreo de Redes y Sistemas F-STE-10 Informe Mensual Monitoreo.	
A.8.7	Protección contra malware	Tecnológico	X				PO-STE-01 Política de SI y Ciberseguridad P-STE-29 Gestión y Configuración de Antivirus y EDR. P-STE-09 Respuesta ante incidentes de SI G-STE-02 Configuración Segura.	
A.8.8	Gestión de vulnerabilidades técnicas	Tecnológico	X				P-STE-30 Gestión de Vulnerabilidades. P-STE-05 Actualización de Software y Parches. F-STE-12 REGISTRO DE VULNERABILIDADES Y PLAN DE REMEDIACIÓN	
A.8.9	Gestión de la configuración	Tecnológico		X			P-STE-31 Gestión de Configuración Segura. G-STE-02 Estándar de Configuración por Tipo de Activo. P-STE-16 Instalación y Configuración de Equipos TI	Se recomienda implementar una herramienta de gestión de configuración, como Ansible o SCCM, que permita automatizar la verificación, aplicación y seguimiento de las configuraciones base (baseline) definidas por la organización. Esto facilitará la estandarización de los entornos tecnológicos, reducirá errores derivados de intervenciones manuales, permitirá identificar desviaciones de manera oportuna y fortalecerá el cumplimiento de los controles de seguridad establecidos.
A.8.10	Eliminación de información	Tecnológico	X				P-STE-32 Eliminación y Disposición Segura. F-STE-13 Registro de Eliminación.	
A.8.11	Enmascaramiento de datos	Tecnológico	X				P-STE-33 Enmascaramiento y Anonimización. G-STE-03 Pseudonimización para Ambientes de Prueba.	
A.8.12	Prevención de fuga de datos	Tecnológico	X				P-STE-34 Prevención de Pérdida de Datos (DLP). PO-STE-01 Política de Seguridad de la Información y Ciberseguridad. (restricciones de transferencia).	
A.8.13	Respaldo de información	Tecnológico	X				P-STE-03 Respaldo y Restauración. P-STE-19 Gestión de Respaldo y Recuperación. L-STE-01 Listado de Rutas Backups	
A.8.14	Redundancia de instalaciones de procesamiento	Tecnológico	X				P-STE-24 Continuidad del Negocio. P-STE-12 Gestión Cloud (Microsoft 365/Azure). P-STE-19 Gestión de Respaldo y Recuperación de Datos	
A.8.15	Registro de actividad (logging)	Tecnológico	X				P-STE-35 Gestión de Logs, Retención y Trazabilidad. P-STE-07 Monitoreo de Redes y Sistemas F-STE-09 Registro Monitoreo Alertas MT-STE-03 Definición de Eventos a Registrar por Sistema.	
A.8.16	Actividades de monitoreo	Tecnológico	X				P-STE-07 Monitoreo de Redes y Sistemas. P-STE-20 Monitoreo y Gestión de Incidentes. F-STE-09 Registro Monitoreo Alertas F-STE-10 Informe Mensual Monitoreo	
A.8.17	Sincronización de relojes	Tecnológico	X				P-STE-07 PROCEDIMIENTO DE MONITOREO DE REDES Y SISTEMAS P-STE-35 Gestión de Logs, Retención y Trazabilidad P-STE-07 Monitoreo de Redes y Sistemas G-STE-02 Configuración Segura (incluye NTP).	
A.8.18	Uso de programas de utilidad con privilegios	Tecnológico	X				P-STE-36 Control de Herramientas y Utilidades Privilegiadas. MT-STE-04 Lista Blanca de Herramientas Privilegiadas. P-STE-26 Gestión de Accesos Privilegiados (PAM)	
A.8.19	Instalación de software en sistemas operativos en producción	Tecnológico	X				P-STE-10 Despliegue de Nuevas Aplicaciones. P-STE-44 Separación de Ambientes. P-STE-06 Gestión de Cambios. P-STE-05 Actualización de Software y Parches P-STE-17 Gestión de Licencias G-STE-06 Checklist Seguridad Software Adquirido	
A.8.20	Seguridad en redes	Tecnológico	X				P-STE-37 Seguridad Perimetral (Firewall/IDS/IPS). P-STE-39 Segregación y Segmentación. G-STE-04 Esquema de Segmentación de Red de Referencia P-STE-07 Monitoreo de Redes y Sistemas P-STE-18 Configuración de Redes Wi-Fi I-STE-01 Instructivo VPN FortiClient & RDP	
A.8.21	Seguridad en los servicios de red	Tecnológico		X			P-STE-38 Gestión de Servicios de Red y Acuerdos con Proveedores MT-STE-05 Inventario de Servicios de Red Contratados. F-CL-01 Acuerdo de Nivel de Servicio (ANS/SLA)	Se recomienda documentar formalmente los acuerdos de niveles de servicio (SLA) relacionados con seguridad y disponibilidad con los proveedores de servicios de red e internet, definiendo responsabilidades, tiempos de respuesta y criterios de escalamiento ante incidentes. Asimismo, es conveniente activar y mantener el monitoreo continuo de disponibilidad y detección de anomalías, registrando los resultados y eventos relevantes en el formato F-STE-09, con el fin de fortalecer la capacidad de respuesta y la continuidad operativa de los servicios.
A.8.22	Segregación de redes	Tecnológico		X			P-STE-39 Segregación y Segmentación de Redes (VLANs, DMZ, Zero Trust). G-STE-04 Esquema de Segmentación de Red de Referencia	Se recomienda incluir dentro del plan de auditoría técnica MT-STE-06 pruebas específicas de verificación de la segregación de redes, con el fin de validar la efectividad de los controles implementados y confirmar que los diferentes segmentos operen conforme a la arquitectura definida. Asimismo, es importante registrar los resultados obtenidos, documentar los desvíos o hallazgos identificados y definir las acciones de seguimiento correspondientes para su tratamiento y cierre.
A.8.23	Filtrado web	Tecnológico	X				P-STE-40 Control y Filtrado de Contenido Web.	
A.8.24	Uso de criptografía	Tecnológico	X				P-STE-41 Gestión Criptográfica y de Claves. G-STE-05 Estándar de Algoritmos y Longitudes de Clave (KeePass AES-256).	

A.8.25	Ciclo de vida de desarrollo seguro	Tecnológico				X	[EXCLUIDO] Berrut no desarrolla software. P-STE-15 Desarrollo y Gestión de Proyectos. G-STE-07 Arquitectura Segura (Security by Design). P-STE-44 Separación de Ambientes.	
A.8.26	Requisitos de seguridad en aplicaciones	Tecnológico				X	[EXCLUIDO] Berrut no desarrolla software. G-STE-06 Checklist Requisitos de Seguridad para Software Adquirido. F-STE-17 Checklist de Seguridad.	
A.8.27	Principios de arquitectura de sistemas seguros	Tecnológico				X	[EXCLUIDO] Berrut no desarrolla software. G-STE-07 Principios de Arquitectura Segura (Security by Design, Defense in Depth). G-STE-04 Segmentación.	
A.8.28	Codificación segura	Tecnológico				X	[EXCLUIDO] Berrut no desarrolla software. P-STE-15 Desarrollo y Gestión de Proyectos. G-STE-07 Arquitectura Segura.	
A.8.29	Pruebas de seguridad en desarrollo y aceptación	Tecnológico				X	[EXCLUIDO] Berrut no desarrolla software. P-STE-43 Pruebas de Aceptación de Seguridad (VAPT). F-STE-17 Checklist Seguridad Software.	
A.8.30	Externalización del desarrollo	Tecnológico				X	[EXCLUIDO] Sin actividad de desarrollo propio ni externalizado.	
A.8.31	Separación de entornos desarrollo, prueba y producción	Tecnológico		X			P-STE-44 Separación Formal de Ambientes (Pre-producción/Producción).	Se recomienda verificar periódicamente la adecuada separación de los ambientes tecnológicos (desarrollo, pruebas y producción), garantizando que existan controles que eviten interferencias o accesos no autorizados entre ellos. Asimismo, es importante documentar la configuración de cada ambiente por proyecto, con el fin de asegurar la trazabilidad, facilitar la gestión de cambios y reducir riesgos operativos y de seguridad.
A.8.32	Gestión de cambios	Tecnológico		X			P-STE-06 Gestión de Cambios en el Entorno de TI. P-STE-04 Formato RFC. P-SGI-02 Procedimiento Gestión del Cambio	Aunque actualmente la gestión se desarrolla a través de GLPI, se recomienda fortalecer el control del proceso mediante la formalización de todos los cambios realizados en la infraestructura de los clientes, asegurando que cuenten con una aprobación previa debidamente documentada y que los registros asociados sean completos, trazables y conservados como evidencia de la autorización y ejecución de cada intervención.
A.8.33	Información de prueba	Tecnológico		X			G-STE-03 Pseudonimización para Ambientes de Prueba. P-STE-33 Enmascaramiento y Anonimización de Datos	Se recomienda verificar en cada proyecto que los datos utilizados para pruebas hayan sido debidamente anonimizados o pseudonimizados, especialmente cuando provengan de información real o sensible. Adicionalmente, es importante mantener registros que evidencien la herramienta empleada y la metodología aplicada para dicho proceso, garantizando la protección de la información, la trazabilidad de las actividades realizadas y el cumplimiento de los requisitos de privacidad y seguridad establecidos.
A.8.34	Protección de sistemas durante pruebas de auditoría	Tecnológico				X	P-STE-45 Auditorías Técnicas y Pruebas de Penetración (En revisión) MT-STE-06 Plan Auditoría Seguridad Técnica (revisión)	Asegurar que las pruebas de penetración sean realizadas por personal independiente con alcance, reglas de compromiso y autorización formal.
NIVEL DE CUMPLIMIENTO — CATEGORÍA A.8			20	6	1	7	85,2%	

CUADRO RESUMEN DE CUMPLIMIENTO — ANEXO A ISO/IEC 27001:2022						
Categoría	Descripción	Cumple	Cumple Parcialmente	No Cumple	No Aplica	% Cumplimiento
A.5	Organizacional (37 controles)	26	11	0	0	85,1%
A.6	Personas (8 controles)	8	0	0	0	100,0%
A.7	Físico (14 controles)	9	2	0	3	90,9%
A.8	Tecnológico (34 controles)	20	6	1	7	85,2%

CUMPLIMIENTO POR CAPÍTULO — CLÁUSULAS 4 AL 10						
Capítulo	Nombre	Cumple	Cumple Parc.	No Cumple	No Aplica	% Cumplimiento
Capítulo 4	Contexto	4	0	0	0,0%	100,0%
Capítulo 5	Liderazgo	3	1	0	0,0%	87,5%
Capítulo 6	Planificación	5	0	0	0,0%	100,0%
Capítulo 7	Soporte	5	0	0	0,0%	100,0%
Capítulo 8	Operación	4	0	0	0,0%	100,0%
Capítulo 9	Evaluación del Desempeño	0	2	2	0,0%	25,0%
Capítulo 10	Mejora	1	2	0	0,0%	66,7%
PROMEDIO GENERAL SGI		3,142857143	0,714285714	0,285714286	0	82,7%

PROMEDIO DEL CAPÍTULO 4 AL 8	97,5%
------------------------------	-------

CUMPLIMIENTO POR CATEGORÍA — ANEXO A (93 CONTROLES ISO 27001:2022)						
Categoría	Descripción	Cumple	Cumple Parc.	No Cumple	No Aplica	% Cumplimiento
A.5	Organizacional (37 controles)	26	11	0	0	85,1%
A.6	Personas (8 controles)	8	0	0	0	100,0%
A.7	Físico (14 controles)	9	2	0	3	90,9%
A.8	Tecnológico (34 controles)	20	6	1	7	85,2%
PROMEDIO GENERAL ANEXO A		15,75	4,75	0,25	2,5	90,3%

INSTRUCCIONES DE USO DE LA MATRIZ
1. En la hoja 'Cláusulas 4-10': marque con X la columna que corresponda para cada requisito.
2. En la hoja 'Anexo A — Controles': marque con X la columna que corresponda para cada control.
3. Solo marque UNA columna por fila (C, CP, NC o NA). El sistema calcula % automáticamente.
4. Al final de cada capítulo/categoría verá el % de cumplimiento calculado.
5. Este Dashboard actualiza los gráficos radiales automáticamente.
Fórmula: % = (Cumple+1 + Cumple Parc.+0.5) / (Total - No Aplica) * 100

