CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Visión de Procesos de Ciberseguridad

Workshop N°1

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

Agenda

- Visión de Procesos en Ciberseguridad
- Procesos de Gobierno y Gestión en un SGSI
- Procesos de Soporte a un SGSI
- Procesos Operativos de Seguridad de la Información y Ciberseguridad
- Reflexiones

Profesor

Carlos Lobos de Medina

Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional de la Universidad de Chile.

Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.}

https://www.linkedin.com/in/clobos/

Visión de Procesos en Ciberseguridad

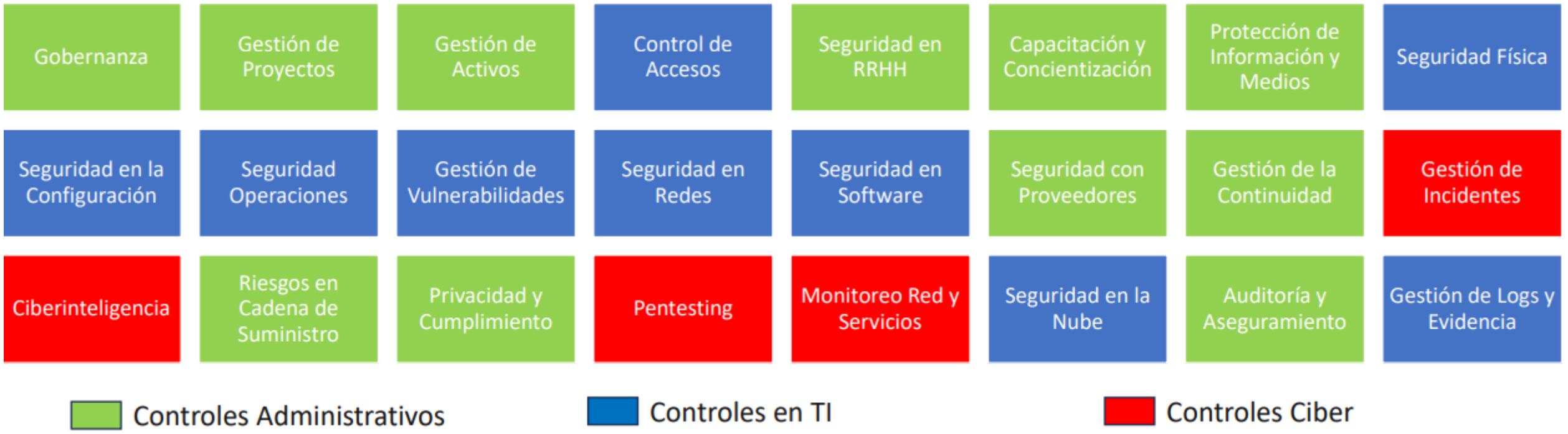
Procesos o Controles de Seguridad de la Información

CIS Controls Version 8
Inventario y Control de los Activos Empresariales
Inventario y Control de Activos de Software
Protección de los Datos
Configuración Segura de Activos y Software Empresarial
Administración de Cuentas
Gestión de Control de Accesos
Gestión Continua de Vulnerabilidades
Gestión de Registros de Auditoría
Protección del Correo Electrónico y Navegador Web
Defensas contra Malware
Recuperación de Datos
Gestión de la Infraestructura de Red
Monitoreo y Defensa de la red
Concientización en Seguridad y Formación de Habilidades
Gestión de Proveedores de Servicios
Seguridad en el Software de Aplicación
Gestión de Respuesta a Incidentes
Pruebas de Penetración

ISO 27002:2022 Controles de Seguridad de la Información
Gobernanza
Gestión de Activos
Protección de Información
Seguridad en Recursos Humanos
Seguridad Fisica
Seguridad en Sistemas y Redes
Seguridad en Aplicaciones
Seguridad en la Configuración
Gestión de Identidades y Accesos
Gestión de Amenazas y Vulnerabilidades
Continuidad del Negocio
Seguridad en las Relaciones con Proveedores
Legal y Cumplimiento
Gestión de Eventos de Seguridad de la Información
Aseguramiento de la Seguridad de la Información
Inteligencia de Amenazas
Seguridad en la Nube
Privacidad y protección de PII
Gestión de Proyectos
Protección de Información

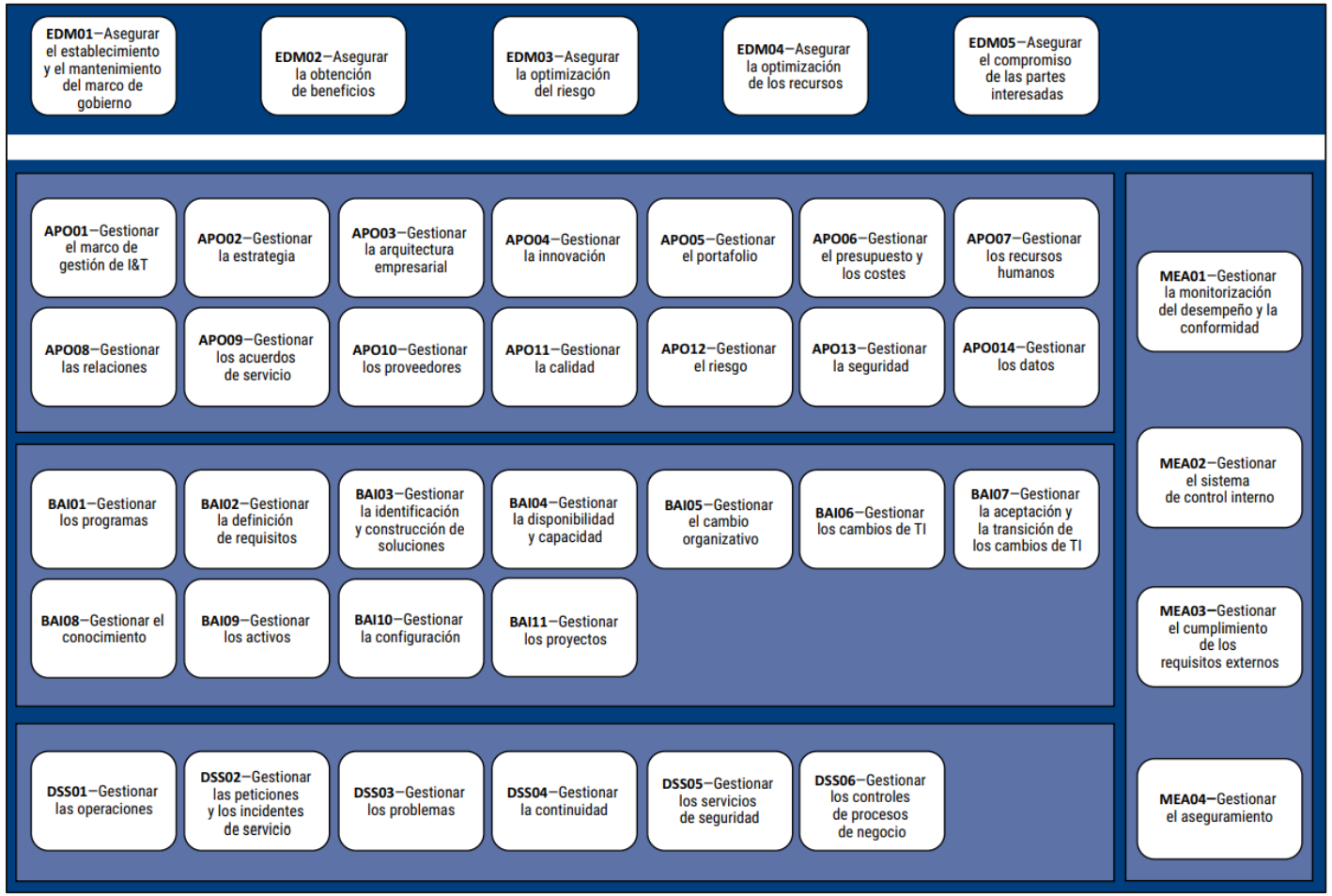
NIST SP 800-53 Revision 5
Control de Accesos
Concientización y Entrenamiento
Auditoría y Accountability
Evaluación, Autorización y Monitoreo de la Seguridad
Gestión de la Configuración
Planificación de la Contigencia
Identificación y Autenticación
Respuesta a Incidentes
Mantención
Protección de Medios
Protección Fisica y del Entorno
Planificación
Gestión del Programa
Seguridad del Personal
Transparencia y Procesamiento de PII
Evaluación de Riesgos
Adquisición de Sistemas y Servicios
Protección de Sistemas y Comunicaciones
Integridad de la Información y Sistemas
Gestión de Riesgos en la Cadena de Suministros

Procesos o Controles de Seguridad de la Información

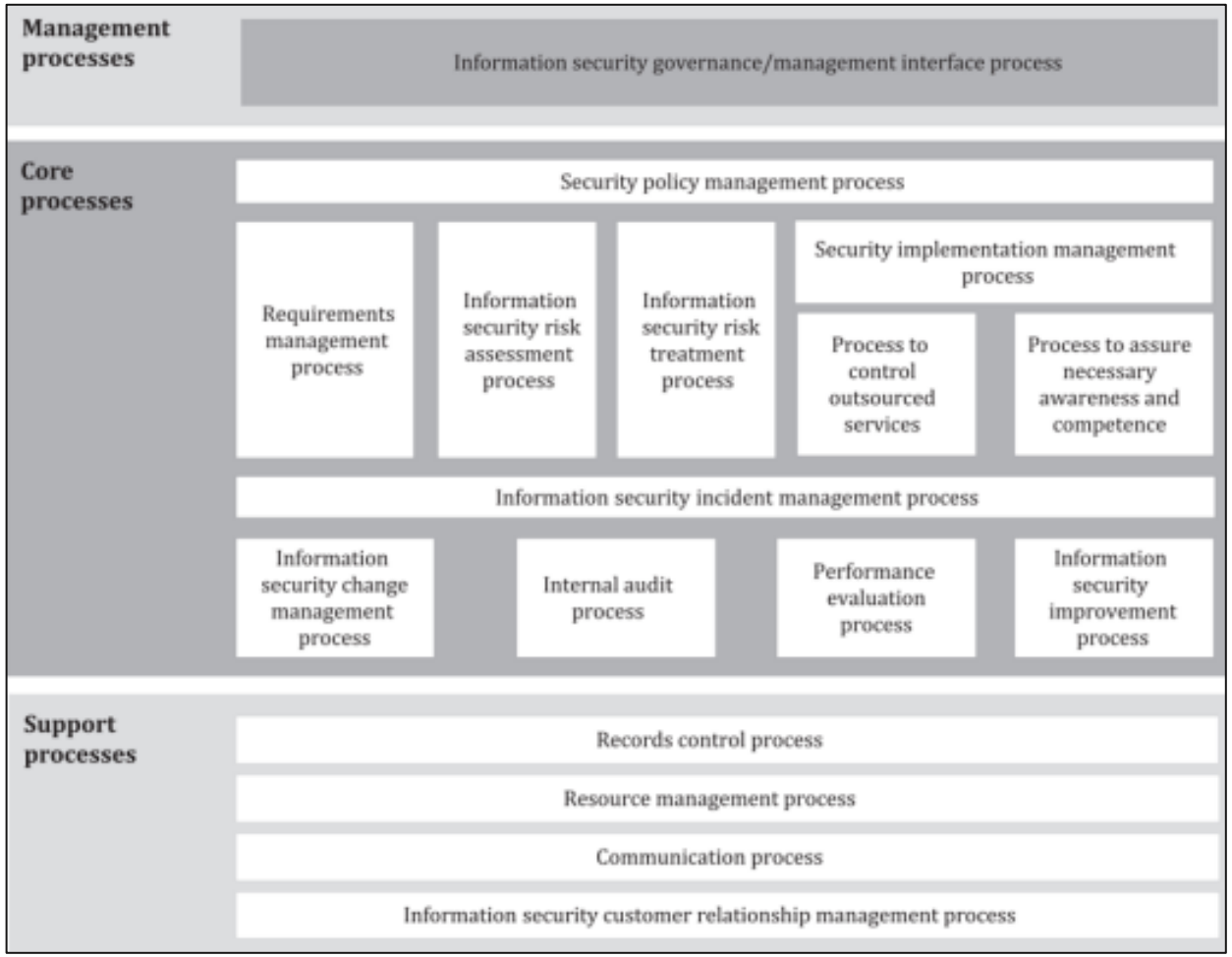


Resumen de controles desde ISO 27002, Cis Control y NIST 800 53

Procesos o Controles de IT – Cobit 2019

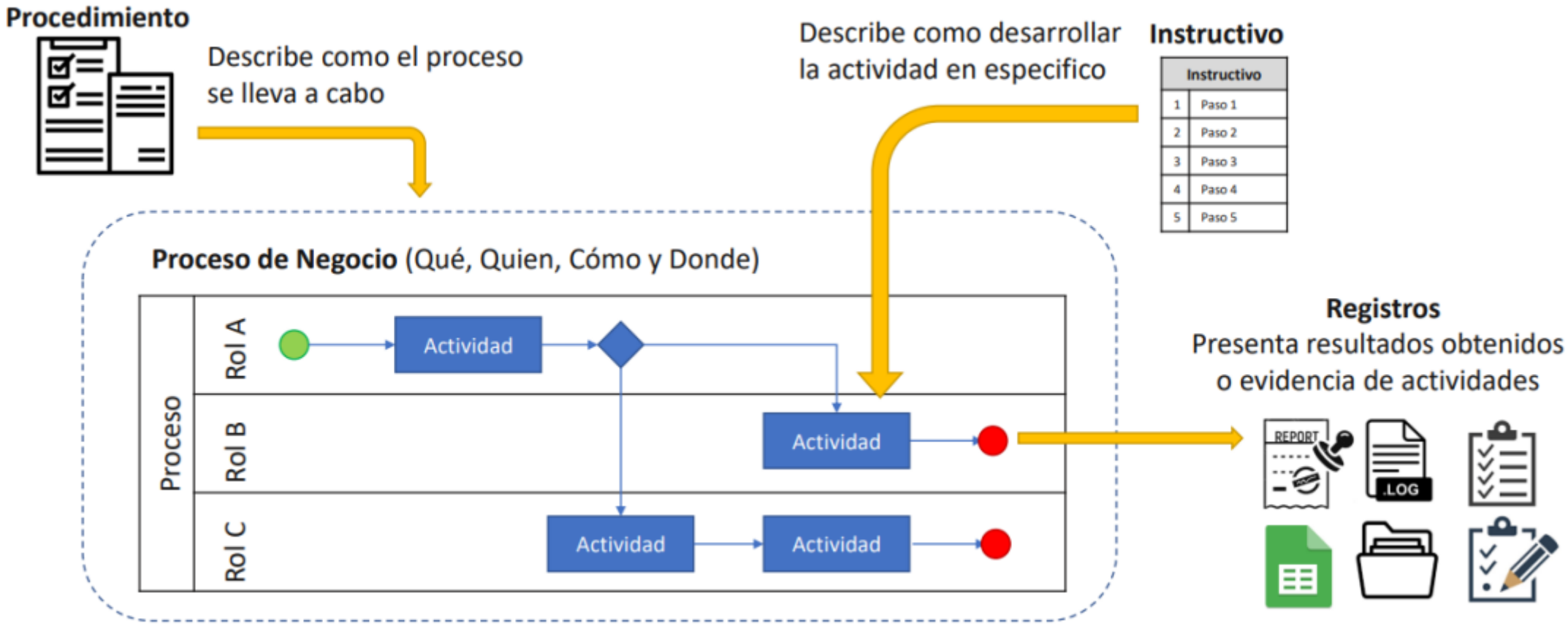


La visión de Procesos SGSI – ISO 27022



- Excelente punto de partida para la implementación de un SGSI
- Pero es un poco tedioso y agregas muchas definiciones innecesaria a los procesos
- Si fuese así nada más deberíamos tener a lo menos 17 procesos para solo administrar el SGSI.
- Que pasa con los procesos más operativos, tecnológicos y de ciberseguridad

Como implementar un proceso



Consideración Importante – ISO 27002 Control 5.37

- Plantea características y definiciones para los procedimientos.

¿Cuando Documentar?

- Cuando se requiera que la actividad se realice de igual forma
- Cuando la actividad se realiza raramente y es probable que sea olvidado la próxima vez
- cuando la actividad sea nueva y presente un riesgo si no se realiza correctamente;
- Antes del traspaso de la actividad al nuevo personal.

¿Que Documentar?

Las personas responsables	Instalación y configuración segura	Procesamiento y manejo de información	Respaldo y resiliencia
Planificación de requisitos	Instrucciones para el manejo de errores	Contactos de soporte y escalamiento	Instrucciones de manejo de medios de almacenamiento
Procedimientos de reinicio y recuperación del sistema	Registros de auditoría y del sistema	Procedimientos de monitoreo (capacidad, desempeño y seguridad)	Instrucciones de mantenimiento

Procesos de Administrativos de un SGSI

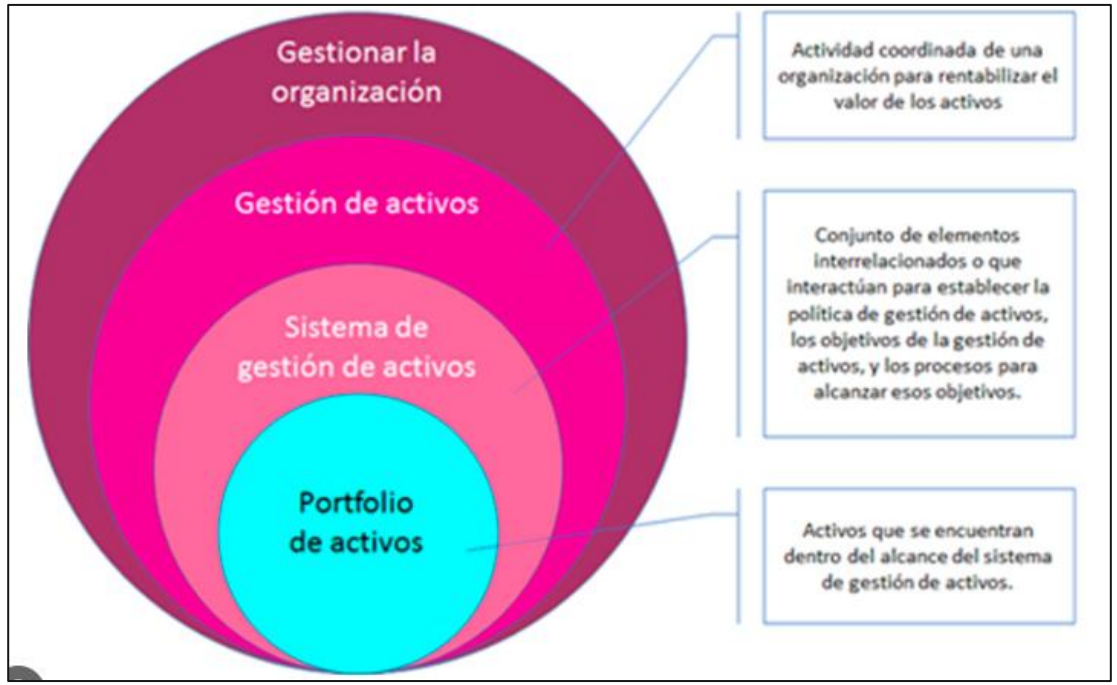
Proceso de Gestión de Activos

- Identificar, clasificar y mantener controlados todos los activos que soportan la operación y la información del negocio.
- Establecer responsables (dueños) de la protección y ciclo de vida de cada activo.
- Permitir la gestión de riesgos basada en criticidad y valor del activo.
- Asegurar el uso adecuado, almacenamiento responsable y eliminación segura de activos.
- Integrar activos con otros procesos: inventario → riesgos → continuidad → accesos → incidentes.
- Mantener una visión dinámica: activos cambian, se crean, migran, se integran y se retiran

Etapa	Descripción	Resultado esperado	Evidencias / Medios de Verificación
1. Identificación de Activos	Detectar información, hardware, software, servicios cloud y proveedores asociados.	Inventario inicial completo.	Lista de activos, plantillas de inventario, registros de descubrimiento automático.
2. Clasificación y Etiquetado	Clasificar activos según **sensibilidad** y **criticidad** (impacto CIA + continuidad).	Matriz de clasificación y etiquetas de seguridad.	Política de clasificación, etiquetas, documentación de niveles (p.ej. Público / Interno / Confidencial).
3. Asignación de Propietarios	Designar **dueños del activo** responsables de su protección y decisiones.	Roles y responsabilidades documentadas.	Matriz RACI, registro de custodios y owners.
4. Gestión de Ciclo de Vida	Controlar altas, cambios, transferencias y bajas seguras.	Procedimiento formal aplicado.	Formatos de alta/baja, registros de movimiento, autorizaciones de cambio.
5. Protección y Mantenimiento	Aplicar medidas de seguridad según clasificación del activo.	Controles adecuados aplicados.	Hardening, cifrado, backups, controles de acceso, logs.
6. Eliminación o Destrucción Segura	Asegurar que activos (incluyendo datos) se destruyen sin dejar residuales.	Cierre de ciclo sin riesgo residual.	Certificados de destrucción, logs de eliminación, cierre de accesos.

Proceso de Gestión de Activos

Marco	Control / Sección	Qué exige
ISO 27001:2022	A.5.9 – A.5.13 (Gestión de activos y propiedad)	Inventario, propiedad, clasificación y manejo seguro.
ISO 27002:2022	**Controles 5.9 a 5.13** detallan cómo hacerlo en práctica	Roles, etiquetado, medios removibles, eliminación.
CIS Controls v8.1	**Control 1 & 2** → Inventario de hardware y software	Descubrimiento, monitoreo continuo, actualización dinámica.
NIST SP 800-53 r5	**CM-8 / MP-6 / SI-12**	Gestión del inventario, medios y vida útil.
COBIT 2019	**BAI09 / DSS01 / DSS05**	Control de configuraciones, activos y operación segura.



ISO 55001

Proceso de Gestión de Proveedores

- Asegurar que los proveedores que acceden procesan o almacenan información cumplan los niveles de seguridad requeridos por la organización.
- Evaluar y gestionar riesgos en la cadena de suministro digital, considerando dependencias críticas.
- Formalizar requisitos contractuales, responsabilidades, obligaciones y niveles de servicio.
- Supervisar el cumplimiento continuo de los proveedores mediante monitoreo y auditorías.
- Establecer mecanismos de terminación segura (devolución o destrucción de datos).Proteger la organización contra incidentes originados en terceros.

Etapa	Descripción	Resultado esperado	Medios de Verificación / Evidencias
1. Identificación y Clasificación de Proveedores	Determinar qué proveedores son críticos según impacto en el negocio y tratamiento de información.	Listado de proveedores clasificados por criticidad.	Inventario de proveedores, matriz de criticidad, mapa de servicios dependientes.
2. Evaluación de Riesgos del Proveedor	Evaluar madurez de seguridad, cumplimiento legal, privacidad y continuidad.	Informe de riesgo del proveedor + decisión de aceptación/mitigación.	Checklists de evaluación, cuestionarios SIG-Lite/CSA, análisis documentado.
3. Formalización Contractual	Incorporar cláusulas de seguridad, privacidad, confidencialidad y retención.	Contratos actualizados con anexos de seguridad.	Contrato firmado, NDA, ANS/SLA, Anexos de tratamiento de datos (DPA).
4. Onboarding Seguro del Proveedor	Gestionar accesos, cuentas, intercambio de datos y especificaciones técnicas.	Alta controlada y trazable en sistemas y procesos.	Registros de accesos concedidos, configuraciones, autorizaciones y aprobaciones.
5. Monitoreo y Seguimiento del Proveedor	Verificar que el proveedor mantiene controles y niveles de servicio acordados.	Supervisión continua y periódica basada en criticidad.	Informes de desempeño, auditorías, KPI de servicio, revisión de incidentes reportados.
6. Gestión de Incidentes del Proveedor	Coordinar detección, comunicación y contención conjunta.	Notificación y manejo integrado del incidente.	Registro de incidentes, análisis causa raíz, reportes compartidos, evidencias de respuesta.
7. Terminación y Desvinculación (Exit)	Finalizar la relación asegurando la **eliminación o devolución de datos** y cierre de accesos.	Proveedor desvinculado sin riesgos residuales.	Certificados de destrucción, logs de cierre de accesos, acta de término.

Proceso de Gestión de Proveedores – Desde Cobit APO10

B. Componente: Estructuras organizativas													
Práctica clave de gestión	Director de riesgos	Director de TI	Director de tecnología	Director de tecnologías digitales	Consejo de gobierno de I&T	Comité de riesgos empresariales	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de Servicios	Gestor de seguridad de la información	Director de privacidad	Asesor legal
APO10.01 Identificar y evaluar los contratos y las relaciones con los proveedores.		R	R	R	A				R				R
APO10.02 Seleccionar proveedores.		R	R	R	A		R	R	R	R	R	R	
APO10.03 Gestionar los contratos y las relaciones con los proveedores.		R	R	R	A		R	R	R	R			R
APO10.04 Gestionar los riesgos de los proveedores.	R	R	R	R	A	R	R	R	R	R	R	R	
APO10.05 Supervisar el rendimiento y el cumplimiento del proveedor.	R	R	R	R	A	R	R	R	R	R			R

Proceso de Gestión de Proveedores

Marco	Sección / Control	Qué exige
ISO 27001:2022	A.5.19–A.5.22 (Relaciones con proveedores, monitoreo, contratos)	Gestión integral de seguridad en proveedores.
ISO 27002:2022	5.19 – 5.23	Detalla cómo evaluar, acordar y controlar riesgos en terceros.
ISO 27701 (Privacidad)	7.2.6 & 8.2.6	Obligación de **equivalencia de controles** en encargados de datos.
CIS Controls v8.1	**Control 15 – Service Provider Management**	Inventario → evaluación → contratos → monitoreo.
NIST SP 800-53 r5	**SR-1 a SR-11 (Supply Chain Risk Management)**	SCRM formal y evidencia continua.
COBIT 2019	**BAI03** (Adquisición), **BAI05** (Cambios), **DSS01** (Operación)	Gobernanza de proveedores alineada a TI y negocio.

Ley	Artículos relevantes
Ley Marco de Ciberseguridad	Modelo de gestión de riesgos y **continuidad** sobre servicios esenciales y servicios tercerizados críticos.
Ley 21.719 (Protección de Datos)	Art. 35–41 (régimen de encargados de tratamiento)

La ISO 27002 ofrece un importante chek list para la gestión de proveedores

Proceso de Gestión de Continuidad del Negocio

- Asegurar la recuperación y continuidad de los servicios críticos frente a incidentes disruptivos.
- Proteger la confidencialidad, integridad y disponibilidad de la información durante contingencias.
- Minimizar impactos financieros, reputacionales, operacionales y regulatorios.
- Establecer planes, roles y procedimientos claros para responder y recuperar en tiempos aceptables.
- Alinear la continuidad con las prioridades estratégicas del negocio (procesos críticos).
- Garantizar la resiliencia, no solo la recuperación: capacidad de resistir, adaptarse y aprender.

Control 5.30 ISO 27002 - Preparación de las TIC para la| continuidad del negocio

- Cambio en fondo muy relevante, con mucho más foco en la gestión de la continuidad de las TIC, antes era difuso y orientado a la continuidad de la Seguridad de la Información

Análisis del Impacto en el Negocio (BIA)

- Definir esquema de Impacto
- Determinar el impacto en el tiempo
- Priorizar en base al impacto los procesos
- Determinar los recursos necesarios
- Establecer RTO y RPO

Desarrollar Estrategias

- Basado en el análisis de riesgo y el BIA
- Puede ser una o mas alternativas
- Definir planes de continuidad

Control 5.30 ISO 27002 - Preparación de las TIC para la| continuidad del negocio

- La organización debe asegurarse

Estructura Organizacional	Capacidades del personal	Planes de continuidad de TIC	Procedimientos de respuesta y recuperación
Ejercicios y pruebas	Aprobación por la Dirección	BCP alineados con el BIA	RTO de cada servicio TIC priorizados
	RPO de cada servicio TIC priorizados	Procedimientos de recuperación	

Proceso de Gestión de Continuidad del Negocio

Etapa	Descripción	Resultados esperados	Medios de Verificación / Evidencias
1. Alcance y Gobierno del Proceso	Definir los procesos, servicios, sistemas y sedes a incluir. Asignar responsables y estructura de gobernanza.	Alcance documentado y roles designados (Comité de Crisis o Continuidad).	- Documento de alcance aprobado - Nombramiento de responsables (RACI) - Actas de comité de continuidad - Organigrama funcional de crisis
2. Análisis de Impacto al Negocio (BIA)	Identificar procesos críticos, recursos necesarios y dependencias. Determinar impacto por interrupción y tolerancias.	Matriz BIA con: procesos críticos, impacto, **RTO/RPO**, MTD.	- Documento de BIA completo - Matriz de criticidad y dependencias - Validación con dueños de proceso - Evidencia de aprobación por dirección
3. Evaluación de Riesgos Disruptivos	Analizar amenazas (físicas, tecnológicas, humanas, ciber), vulnerabilidades y escenarios de falla.	Matriz de riesgo de continuidad, priorización de amenazas y escenarios.	- Matriz de riesgos (con probabilidad e impacto) - Escenarios documentados - Reporte de revisión conjunta Seguridad + Operaciones
4. Definición de Estrategias de Continuidad	Determinar cómo mantener o restaurar capacidad operacional (sitio alterno, redundancia, backup cloud, operación degradada).	Estrategia de continuidad aprobada y financiada.	- Documento de estrategia de continuidad - Costeo/ROI asociado - Acta de aprobación de la Dirección - Evidencias de contratos o capacidades disponibles
5. Desarrollo de Planes (BCP/DRP)	Redactar planes operativos por proceso y por plataforma tecnológica. Integrar roles, comunicaciones y procedimientos.	Plan de Continuidad (BCP) y Plan de Recuperación Tecnológica (DRP) versionados.	- BCP y DRP en repositorio controlado - Procedimientos paso a paso - Listado de contactos críticos - Versionado y control documental (firma / código / fecha)
6. Pruebas, Simulaciones y Ejercicios	Realizar pruebas de escritorio (tabletop), pruebas técnicas y recuperaciones programadas para validar capacidad real.	Evidencia de efectividad del plan y tiempos de recuperación reales (MTTR vs RTO).	- Informes de pruebas - Registros de resultados y desvíos - Lecciones aprendidas - Planes de acción y seguimiento
7. Revisión, Mejora y Actualización Continua	Ajustar los planes según cambios en infraestructura, personal, proveedores o auditorías. Retroalimentar el SGSI.	Planes vigentes, actualizados y alineados a la estrategia actual.	- Historial de versiones - Fechas de revisión programadas - Evidencias de actualización post incidente o post prueba - Registros de Revisión por la Dirección

Proceso de Gestión de Continuidad del Negocio

Marco	Control / Sección relevante	Qué aporta
ISO 27001:2022	**Cláusula 8.5** Gestión de Continuidad de la Información	Exige que la organización mantenga operación durante incidentes.
ISO 27002:2022	**5.29 y 5.30** (Continuidad y Redundancia)	Define cómo proteger disponibilidad y recuperar operaciones.
ISO 22301:2019 (BCM)	**Cláusulas 8.2 – 8.4** (BIA, Estrategias, Ejercicios)	Marco completo para resiliencia organizacional.
CIS Controls v8.1	**Control 11 – Data Recovery**	Asegura recuperación de datos confiable, probada y segura.
NIST SP 800-53 r5	**CP-1 a CP-10** (Contingencia y recuperación)	Requisitos técnicos para recuperación de servicios e infraestructura.
NIST SP 800-34 r1	**Contingency Planning Guide**	Guía práctica para estructurar planes y pruebas.
COBIT 2019	**DSS04 – Continuidad de Servicio**	Enmarca el gobierno y ciclo de vida de la continuidad.

- 22.300 – Vocabulario
- 22.301 – Requisitos del sistema de gestión de continuidad del negocio
- 22.313 – Directrices de Implementación
- 22.317 – Directrices para el desarrollo del BIA
- 22.320 – Directicas para la respuesta a incidentes
- 22.331 - Directrices para estrategias de continuidad del negocio
- 22.332 – Directrices para la implementación de planes de continuidad
- 22.398 – Directrices para el desarrollo de ejercicios

Proceso de Privacidad y Cumplimiento

Etapa	Descripción	Resultados esperados	Medios de Verificación / Evidencias
1. Identificación y Registro de Tratamientos	Levantar procesos que tratan datos personales (PII) y sus finalidades.	Registro de actividades de tratamiento (RAT).	-Inventario de bases de datos - mapas de datos - flujos de información - clasificación de datos.
2. Base Legal y Consentimiento	Determinar la legitimidad del tratamiento (contrato, obligación legal, interés legítimo, consentimiento).	Matriz de bases legales documentada.	- Cláusulas de consentimiento - avisos de privacidad - registros de aceptación/trazabilidad.
3. Evaluación de Riesgos y EIPD (DPIA)	Evaluar riesgos para titulares cuando existe alto impacto (perfilamiento, biometría, datos sensibles).	EIPD aprobada y registrada.	- Metodología de EIPD - análisis de impacto - decisión y firma del responsable.
4. Privacidad por Diseño y por Defecto	Integrar privacidad en proyectos, sistemas y productos desde el inicio.	Requisitos funcionales de privacidad aplicados en diseño.	- Checklists de diseño - revisiones de seguridad y privacidad - validación de minimización de datos.
5. Gestión con Encargados y Proveedores	Asegurar cumplimiento de terceros que procesan datos personales.	Contratos con cláusulas de privacidad y seguridad equivalentes.	- Evaluación de proveedores - ANSs/SLAs - auditorías - anexos de seguridad y supresión de datos al término.
6. Gestión de Derechos del Titular	Responder solicitudes de acceso, rectificación, portabilidad, oposición o supresión.	Procedimiento y tiempos regulados asegurados.	´-Registros de solicitudes - tiempos de respuesta libro de trazabilidad - evidencia de resolución.
7. Respuesta a Incidentes con Datos Personales	Detectar, contener, documentar y **notificar** brechas cuando corresponda.	Notificación responsable y dentro de plazo legal.	- Registro de incidentes - comunicaciones a titulares y autoridad según severidad. - Lecciones aprendidas
8. Monitoreo, Auditoría y Mejora Continua	Mantener la privacidad como proceso vivo.	Programa anual de revisión.	- Informes de auditoría - indicadores y acciones correctivas documentadas.

Principios Claves de Privacidad – ISO 29100

1. Responsabilidad (Accountability)
2. Limitación de propósito
3. Minimización de datos
4. Calidad y exactitud de datos
5. Limitación de uso, retención y divulgación
6. Seguridad
7. Transparencia y apertura
8. Participación individual y acceso
9. Consentimiento y elección
10. Responsabilidad del tercero receptor
11. Cumplimiento y monitoreo

La ISO 29100 proporciona la arquitectura conceptual del tratamiento ético y legal de los datos personales: define los once principios universales que estructuran la rendición de cuentas, la legitimidad del propósito, la transparencia y la autodeterminación informativa. Su adopción permite traducir los derechos fundamentales de los titulares en políticas coherentes y verificables dentro de cualquier institución pública o privada

Principios ISO 29100 vs Ley PDP

Principio ISO 29100	Concepto central	Ley 21.719	Ley 19.628	Descripción del vínculo normativo	Acciones requeridas
1. Responsabilidad (Accountability)	Rendición de cuentas del responsable.	Art. 3 e), 14 quinquies j)	Art. 11	El responsable debe mantener evidencia verificable del cumplimiento.	- Nombrar Encargado de Protección de Datos (EPD). - Elaborar política institucional de protección de datos. - Crear matriz de cumplimiento legal y técnico. - Reportar anualmente a la Agencia y CAIGG.
2. Limitación de propósito	Fines específicos y legítimos.	Art. 3 b), 14 ter	Art. 12	Los datos deben tratarse solo para los fines informados al titular.	- Incorporar declaración de finalidad en formularios y sistemas. - Registrar finalidades en el ROPA. - Limitar uso secundario o reutilización de datos.
3. Minimización de datos	Solo los datos estrictamente necesarios.	Art. 3 c), 14 ter d)	Art. 10	Los datos deben ser adecuados y proporcionales al propósito.	- Revisar formularios y eliminar campos innecesarios. - Implementar privacidad por defecto en sistemas. - Evaluar bases históricas para eliminar exceso de información.
4. Calidad y exactitud de datos	Exactitud, actualización y pertinencia.	Art. 3 d), 14 quinquies i)	Art. 12 inc. 1°–3°	Los datos deben mantenerse correctos y actualizados.	- Implementar mecanismo de actualización automática o validación anual. - Establecer procedimiento de rectificación de datos.- Monitorear calidad de registros.

Principios ISO 29100 vs Ley PDP

Principio ISO 29100	Concepto central	Ley 21.719	Ley 19.628	Descripción del vínculo normativo	Acciones requeridas
5. Limitación de uso, retención y divulgación	No conservar más tiempo del necesario.	Art. 3 c), 14 ter f)	Art. 18	Se restringe el tiempo de conservación y la comunicación.	- Establecer plazo de eliminación de datos. - Aplicar anonimización para fines estadísticos. - Documentar políticas de retención y destrucción.
6. Seguridad	Protección mediante medidas técnicas y organizativas.	Art. 3 f), 14 quinquies c–f	Art. 11	Exige controles proporcionales al riesgo del tratamiento.	- Implementar política de ciberseguridad institucional - Aplicar controles definidos por la ANCI. - Realizar simulacros de incidentes y brechas.
7. Transparencia y apertura	Comunicación clara al titular.	Art. 3 g), 14 ter	Art. 12 inc. 1°	Se debe informar sobre política, derechos y finalidades.	- Publicar aviso de privacidad institucional. - Incluir información en la web de transparencia activa. - Crear canal de consultas y reclamos.
8. Participación individual y acceso	Acceso, rectificación y eliminación.	Arts. 4–11	Art. 12 completo	Se reconocen derechos ARCO+ ampliados.	- Implementar portal digital de derechos ARCO+. - Definir plazos y responsables de respuesta - Mantener registro de solicitudes.

Principios ISO 29100 vs Ley PDP

Principio ISO 29100	Concepto central	Ley 21.719	Ley 19.628	Descripción del vínculo normativo	Acciones requeridas
9. Consentimiento y elección	Consentimiento libre e informado.	Arts. 12–13	Arts. 4 y 10	Requiere consentimiento previo, salvo excepciones.	- Incorporar checkbox o validación digital de consentimiento. - Guardar evidencia documental. - Revisar excepciones por mandato legal.
10. Responsabilidad del tercero receptor	Obligación de aplicar los mismos principios.	Art. 15 bis, 26	Art. 8	Exige cumplimiento equivalente en terceros o transferencias.	- Actualizar contratos y convenios de datos. - Incorporar cláusulas de confidencialidad y subencargo. - Auditar a terceros y proveedores.
11. Cumplimiento y monitoreo	Auditoría y control del cumplimiento.	Art. 14 quinquies j), 29	Art. 11 y Título II	Requiere control continuo y reportes verificables.	- Realizar auditorías internas anuales (CAIGG). - Preparar informes de cumplimiento para la Agencia. - Implementar indicadores de gestión y tableros PIMS.

Proceso de Privacidad y Cumplimiento

Marco	Control / Cláusula	Qué exige / Enfoque clave
ISO 27001:2022	Cláusula 5 y 6 (liderazgo y planificación), A.5.34–A.5.36 (Privacy)	Integración de privacidad dentro del SGSI.
ISO 27002:2022	5.34 (Protección de PII), 5.35–5.36 (Cumplimiento y protección legal)	Controles concretos de privacidad y evidencia documental.
ISO 27701:2019	Extensión de 27001 para Privacidad (roles PII Controller y PII Processor)	Modelo completo para sistema de gestión de privacidad.
CIS Controls v8.1	Control 15 (Service Provider Management), Control 3 (Data Protection)	Fuerte enfoque en inventario y control de acceso a datos.
NIST SP 800-53 r5 (Privacidad)	**AR-1 a AR-8**, **IP-1 a IP-8**, **PT-1 a PT-8**	Gestión operacional de privacidad + DPIA + derechos titulares.
NIST Privacy Framework (PF)	Core Functions: **Identify–Govern–Control–Communicate–Protect**	Marco operativo para integración con SGSI + arquitectura.
COBIT 2019	**EDM03** (Gestión de riesgo), **APO13** (Gestión de Seguridad), **DSS05** (Protección de Datos)	Privacidad integrada en gobierno corporativo.

Tres normas son claves:
ISO 29100
ISO 27701
ISO 31700

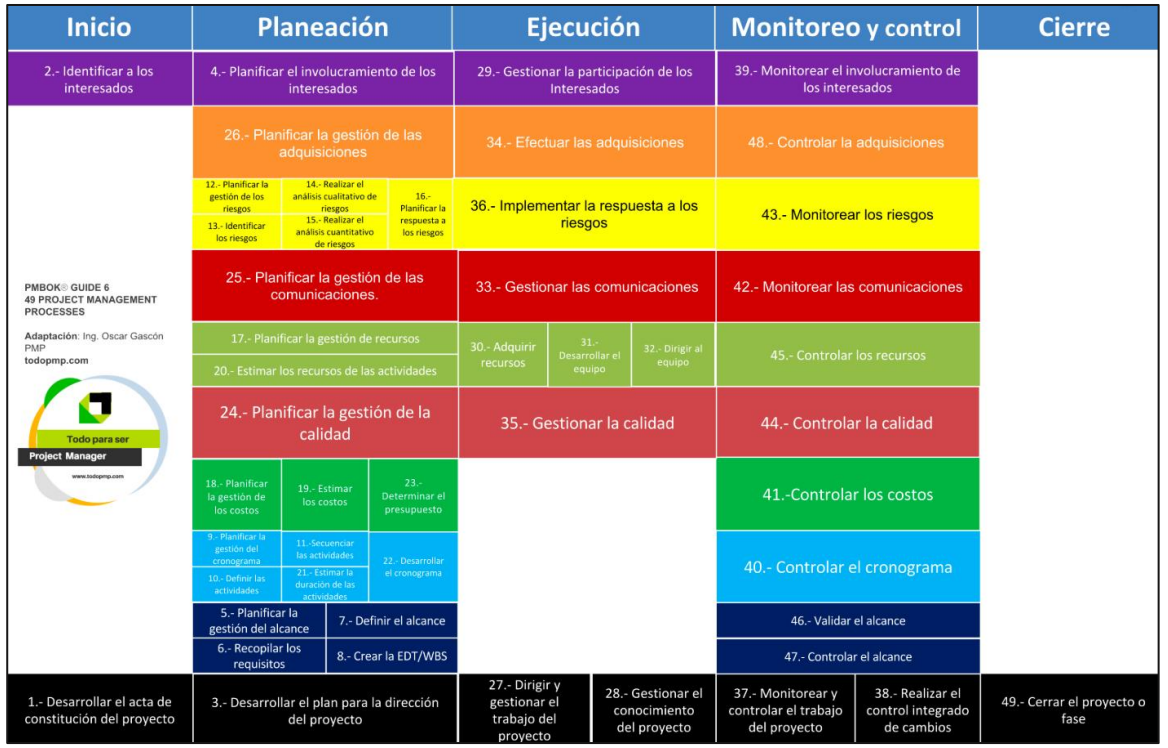
Proceso de Gestión de Proyectos

Etapa	Descripción	Resultados esperados	Medios de Verificación / Evidencias
1. Inicio y Alineamiento Estratégico	Se define la necesidad, justificación y objetivo del proyecto.	Acta de Constitución del Proyecto (Project Charter).	Charter firmado, Sponsor definido, alcance inicial.
2. Planificación Integral del Proyecto	Se establece el plan de trabajo, cronograma, presupuesto y roles.	Plan de Proyecto aprobado.	EDT/WBS, cronograma, matriz RACI, plan de comunicaciones.
3. Identificación y Gestión de Riesgos	Se identifican riesgos operacionales, tecnológicos y de seguridad.	Matriz de Riesgos del Proyecto.	Registro de riesgos, análisis de probabilidad/impacto, plan de respuesta.
4. Diseño y Desarrollo de Entregables	Construcción, adquisición o implementación de soluciones.	Entregables validados y documentados.	Bitácoras de desarrollo, especificaciones, registro de cambios.
5. Control y Monitoreo del Proyecto	Se supervisa avance, calidad, costos, desviaciones y riesgos.	Informes de Avance y Control de Cambios.	KPIs, tablero de control, actas del comité de proyecto, reporte de hitos.
6. Cierre y Transferencia a Operaciones	Se valida cumplimiento de objetivos y se operacionaliza el proyecto.	Informe de Cierre y Lecciones Aprendidas.	Acta de cierre, evaluación contra base, actualización documental.

Momento	Integración de SI	Evidencias esperadas
Inicio	Clasificación del proyecto según riesgo	Ficha de proyecto + Nivel crítico
Planificación	Definición de requisitos de seguridad, privacidad y continuidad	Checklist de requisitos + Matriz de cumplimiento
Riesgos	Identificación y tratamiento de riesgos de SI	Matriz de riesgos (operacionales + TI + ciber)
Desarrollo	Validación técnica de cumplimiento	Registros de revisión técnica / QA
Cierre	Confirmación de operación segura y documentación	Go/No-Go + Lecciones aprendidas

Proceso de Gestión de Proyectos

Marco	Sección / Control relevante	Lo que exige
PMBOK (6ª/7ª Ed.)	Gestión de Integración, Alcance, Riesgos, Stakeholders	Gobernanza, control de riesgos y trazabilidad.
ISO 21502 / ISO 21500	Dirección y gestión de proyectos	Estructura organizacional + ciclo de vida con control.
COBIT 2019	**BAI01 – BAI06** (gestión de programas y proyectos)	Estructura de portafolio, aprobación, arquitectura y control de cambios.
ISO 27001:2022	Cláusula 5 y 6 (gobernanza y planificación del SGSI)	Alineamiento estratégico y roles definidos.
ISO 27002:2022	**5.8, 5.9, 5.31** (seguridad en el ciclo de vida / cumplimiento)	Seguridad integrada a proyectos y adquisiciones.
NIST SP 800-53 r5	**SA-3 a SA-11 / PM-3 / CM-3**	Requisitos de seguridad, arquitectura y gestión de cambios.
CIS Controls v8.1	**Control 4 y 16** (configuración y desarrollo)	Controles mínimos al ingresar nuevos componentes al entorno.



PMBook

5.8 Seguridad de la información en la gestión de proyectos (ISO 27002)

- Las actividades de gestión de proyectos en uso, debería exigir que:
  a) La identificación y gestión de los requisitos de seguridad de la información (por ejemplo, requisitos de seguridad en aplicación (8.26), requisitos para cumplir con los derechos de propiedad intelectual (5.32) y los procesos asociados para los entregables son integrados en las primeras etapas de los proyectos;
  b) Los riesgos de seguridad de la información se evalúan y tratan en una etapa temprana y periódicamente como parte de riesgos del proyecto a lo largo de los ciclos de gestión del proyecto;
  c) Los riesgos de seguridad de la información asociados con la ejecución de proyectos, como la seguridad las comunicación internas y externas se consideran y tratan a lo largo del ciclo de vida del proyecto;
  d) Se realicen pruebas de efectividad del control de seguridad de la información;
  e) La seguridad de la información forma parte de todas las fases de la metodología del proyecto.

5.8 Seguridad de la información en la gestión de proyectos (ISO 27002)

- También se debe considerar lo siguiente al determinar estos requisitos:
  a) Qué información está involucrada (determinación de la información) y cuál es su correspondiente valor (clasificación);
  b) Las necesidades de protección requeridas de la información y otros activos asociados involucrados, particularmente en términos de confidencialidad, integridad y disponibilidad;
  c) El nivel de confianza o seguridad requerido con respecto a la identidad reclamada de las entidades con el fin de derivar los requisitos de autenticación;
  d) Los procesos de aprovisionamiento y autorización de acceso, para clientes y otros usuarios comerciales potenciales, así como para usuarios privilegiados o técnicos, como miembros relevantes del proyecto, operación potencial personal o proveedores externos;
  e) Informar a los usuarios de sus deberes y responsabilidades;
  f) Requisitos derivados de los procesos comerciales, como el registro y seguimiento de transacciones, requisitos de no repudio;
  g) Requisitos exigidos por otros controles de seguridad, por ejemplo interfaces para registro y monitoreo o DLP;
  h) El cumplimiento del entorno legal, estatutario, reglamentario y contractual en el que opera la organización;
  i) Nivel de confianza o seguridad requerida para que terceros conozcan la información de la organización política de seguridad y políticas específicas del tema, incluidas las cláusulas de seguridad relevantes en cualquier acuerdo o preparativos

Gestión de proyectos desde Cobit 2019

B. Componente: Estructuras organizativas											
Práctica clave de gestión	Director general ejecutivo	Director de riesgos	Director de TI	Consejo de gobierno de I&T	Dueños del proceso de negocio	Comité Estratégico (Programas/Proyectos)	Gestor de programas	Oficina de gestión de proyectos	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI
BAI01.01 Mantener un enfoque estándar en la gestión de programas.	A		R	R			R				
BAI01.02 Iniciar un programa.		R			R	A	R	R			
BAI01.03 Gestionar el compromiso de las partes interesadas.					R	A	R	R			
BAI01.04 Desarrollar y mantener el plan del programa.						A	R	R			
BAI01.05 Lanzar y ejecutar el programa.			R		R	A	R	R			
BAI01.06 Monitorizar, controlar y reportar sobre los resultados del programa.			R			A	R	R	R	R	R
BAI01.07 Gestionar la calidad del programa.					R	A	R	R			
BAI01.08 Gestionar el riesgo del programa.		R			R	A	R	R		R	
BAI01.09 Cerrar un programa.			R		R	A	R	R		R	

Procesos Tecnologicos de un SGSI

Proceso de Gestión de Accesos e Identidades

- Garantizar que la identidad digital de usuarios, sistemas y servicios sea gestionada correctamente durante todo su ciclo de vida.
- Asegurar que los accesos se otorguen bajo el principio de mínimo privilegio y necesidad de saber.
- Reducir el riesgo de abuso de cuentas, accesos no autorizados o movimientos laterales.
- Monitorear, revisar y ajustar accesos de forma continua en base a cambios de rol, proyectos o desvinculación.
- Integrarse con la gestión de activos, continuidad, incidentes y auditoría.
- Soportar modelos modernos como Zero Trust, MFA universal y autenticación adaptativa.

Etapa	Descripción	Resultado esperado	Evidencias verificables
1. Creación / Alta de Identidad	Generación controlada de cuentas para usuarios internos, externos o sistemas.	Cuenta creada con rol inicial aprobado.	Solicitud autorizada, ticket, registro en IAM/AD/IdP.
2. Asignación de Roles y Privilegios	Asignar permisos según función, no según persona (**RBAC** o **ABAC**).	Permisos coherentes con rol laboral.	Matriz de roles, RACI, permisos aprobados.
3. Autenticación y Autorización	MFA, certificados, SSO, federación de identidades.	Accesos verificados y auditables.	Evidencia de MFA habilitado, logs de autenticación, tokens.
4. Revisión Periódica de Accesos	Validación trimestral o semestral con dueños de activo/información.	Accesos inconsistentes detectados y revocados.	Registros de revisión, lista de revocación, reportes de compliance.
5. Gestión de Cambios de Rol	Ajustes cuando una persona cambia de función o unidad.	Actualización o reducción de privilegios.	Tickets de cambio, evidencia de remoción/agregado de permisos.
6. Baja / Revocación	Eliminación o deshabilitación de cuentas al finalizar relación contractual.	Cierre total y seguro de la identidad.	Logs de eliminación, auditoría de accesos residuales, retiro de llaves/credenciales.

Proceso de Gestión de Accesos e Identidades

ISO 27002:2022	ISO 27.002:2013	Nombre del Control
5,15	9.1.1, 9.1.2	Control de acceso
5,16	9.2.1	Registro y baja de usuario
5,17	9.2.4, 9.3.1, 9.4.3	Autenticación de información
5,18	9.2.2, 9.2.5, 9.2.6	Derechos de acceso
8,2	9.2.3	Gestión de privilegios de acceso
8,3	9.4.1	Restricción del acceso a la información
8,4	9.4.5	Control de acceso al código fuente de los programas
8,5	9.4.2	Procedimientos seguros de inicio de sesión
8,18	9.4.4	Uso de utilidades con privilegios del sistema

Controles Organizacionales

Controles Tecnológicos

Proceso de Gestión de Accesos e Identidades

DEFINIR LA POLITICA!!!

Intenciones globales y orientación de una organización relativas a la Calidad tal como se expresan formalmente por la Alta Dirección (ISO 9.000)

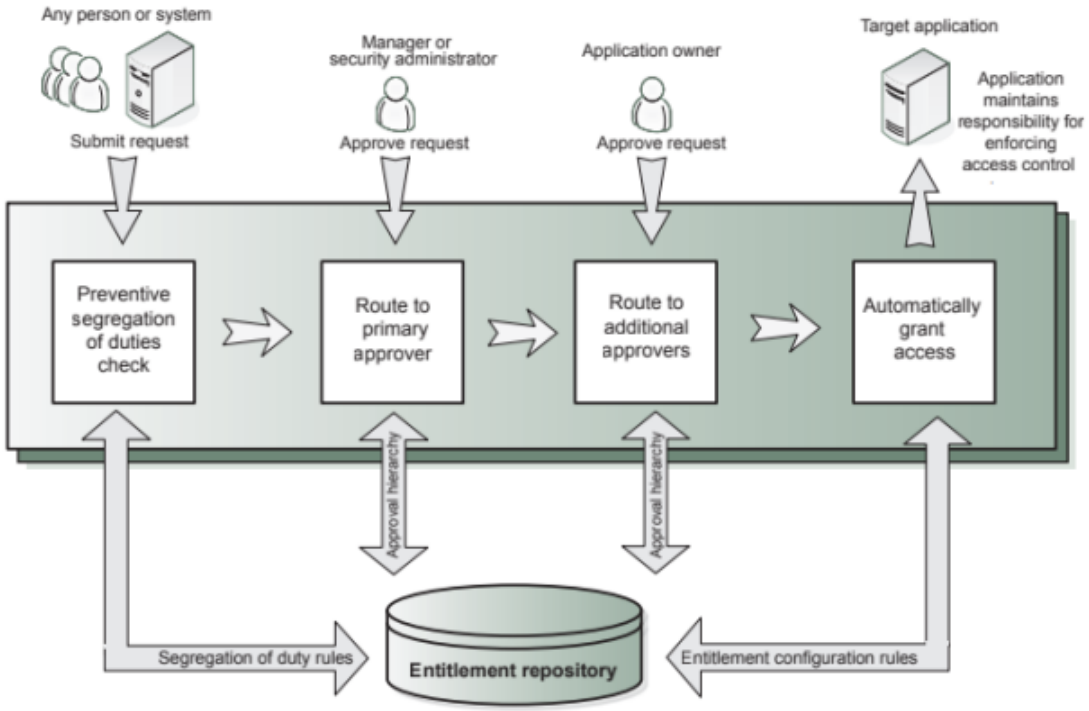
En este contexto

Seguridad de aplicaciones	(8.26)
Acceso Físico	(7.2, 7.3, 7.4)
Autorización y niveles de seguridad	(5.10, 5.12, 5.13)
Restricciones a Accesos privilegiados	(8.2)
Segregación de funciones	(5.3)
Legislación relevante	(5.31)
Segregación de accesos	
Autorización formal de acceso	(5.16, 5.18)
Gestión de accesos	(5.18)
Inicio de sesión	8.15)

5.16 Gestión de la Identidad – actividades a considerar

Se debería tener un proceso:

Otra forma de verlo:



Fuente: GTAG N°9 – The IIA

5.18 Derechos de Accesos

Entrega o revocación de acceso

Para asignar o revocar accesos se debería:

- Obtener Autorización del dueño del activo
- Considerar requisitos de negocio
- Considerar Políticas de Control de Acceso
- Asegurar la eliminación de accesos
- Accesos temporales
- Verificar niveles de accesos
- Mantener un registro de accesos

Proceso de Gestión de Configuración

- Establecer y aplicar configuraciones seguras por defecto (hardening) para sistemas, redes y aplicaciones.
- Reducir la superficie de ataque mediante deshabilitación de servicios, puertos y funciones innecesarias.
- Mantener configuraciones consistentes, documentadas y auditablemente replicables.
- Detectar y corregir cambios no autorizados o desviaciones frente al estándar definido.
- Integrarse con procesos de vulnerabilidades, incidentes, accesos y monitoreo.
- Asegurar trazabilidad completa de configuraciones a lo largo del ciclo de vida del activo.

Etapa	Descripción	Resultado esperado	Evidencias verificables
1. Definición de Configuraciones Baseline	Crear **plantillas estándar de configuración segura** por tipo de activo.	Baselines corporativos aprobados.	Documentos de hardening, guías CIS Benchmarks, plantillas de configuración.
2. Implementación de Configuraciones	Aplicar baseline en la puesta en marcha de servidores, equipos y servicios.	Sistemas instalados de forma segura desde el origen.	Evidencia de instalación, registros de despliegue, imágenes estándar.
3. Control de Cambios (CM)	Asegurar que cualquier modificación esté autorizada y registrada.	Cambios trazables, reversibles y aprobados.	Tickets de cambio, bitácoras, aprobaciones, matriz RACI.
4. Monitoreo de Configuración (CMDB / Detección de Desviaciones)	Detectar alteraciones respecto al baseline.	Alertas ante cambios no autorizados.	CMDB actualizada, reportes de desviación, herramientas de configuración/SCM.
5. Auditoría y Validación Periódica	Verificar cumplimiento del estándar en ambiente real.	Cumplimiento demostrable y documentado.	Checklists, reportes de auditoría interna, dashboards de conformidad.
6. Corrección y Mejora Continua	Ajustar configuraciones en función de nuevas amenazas o lecciones aprendidas.	Baselines actualizados y mejoras aplicadas.	Versiones documentadas, control de cambios de baseline, historial de ajustes.

8.9 Gestionar la Configuración

Témplate base:

- Usar configuraciones bases de los vendors
- Determinar nivel de protección alineado al negocio
- Considerar la factibilidad y aplicabilidad
- Deshabilitar identidades innecesarias, no utilizadas o inseguras;
- Deshabilitar o restringir funciones y servicios innecesarios
- Restringir accesos y uso de programas superprivilegiados
- Sincronizar relojes
- Cambio de autentificación por defecto
- Cierre de sesiones por periodo de inactividad
- Verificación de condiciones de licenciamiento

Gestionar la configuración

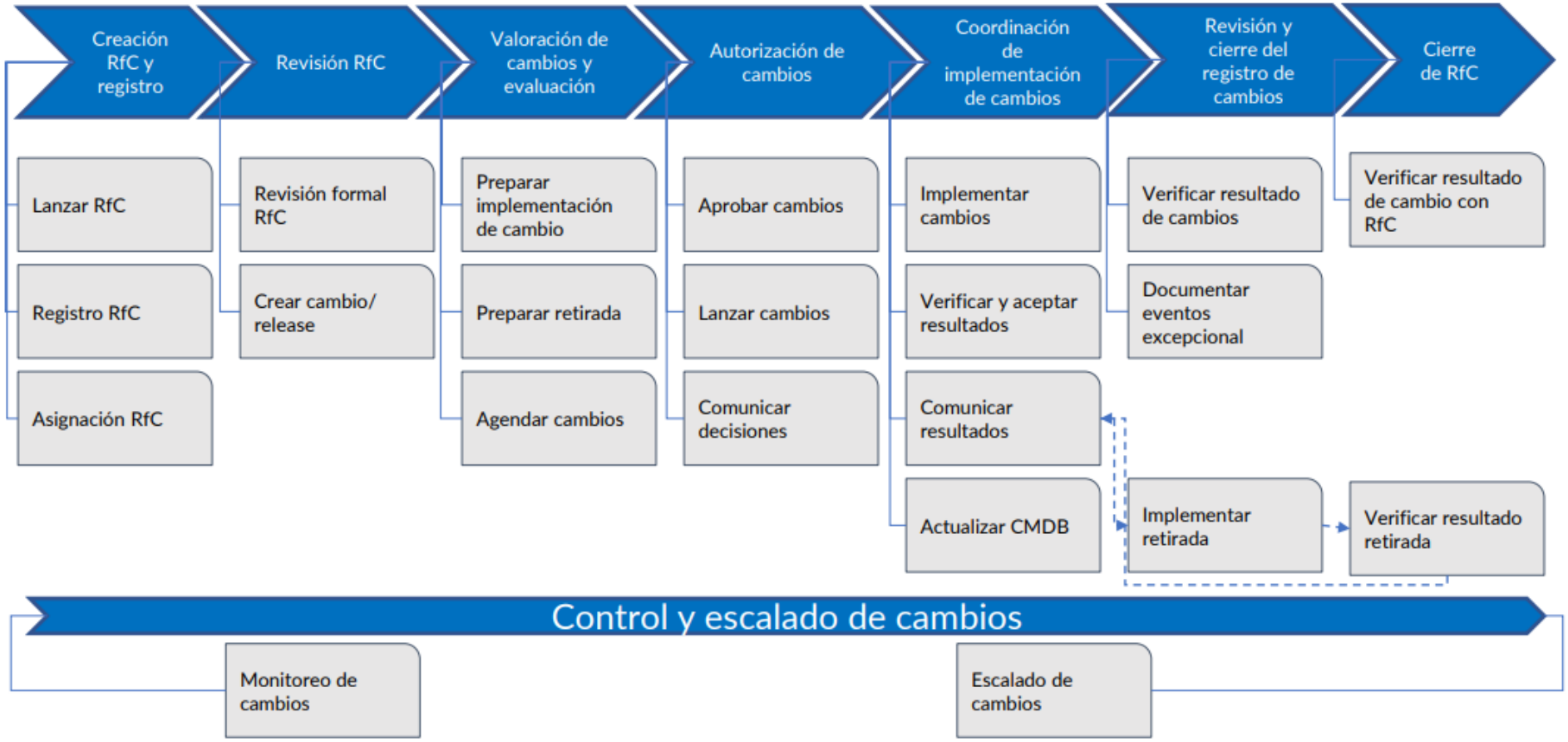
- Información actualizada
- Identificación de propietario y/o punto de contacto
- Control de cambios
- Versionamiento de plantillas de configuración
- Relación con configuraciones de otros activos

8.1 Dispositivo de Usuario Final - General

Debería considerarse la realización de una política, la cual contenga:

- Clasificar de acuerdo a la información
- Registro de usuarios de Endpoint
- Requisitos de seguridad física
- Restricciones de instalación de software
- Actualización Automática de software
- Reglas para conectarse a redes
- Control de acceso
- Discos cifrados
- Protección contra malware
- Gestión de Accesos remotos
- Respaldos
- Uso de servicios web y aplicaciones
- Analítica de comportamiento
- Uso de dispositivos móviles

Gestionar el Cambio - ITIL



8.32 Gestión del Cambio

- Control bastante general y similar a lo establecido en la versión anterior.

Planificar y evaluar el impacto potencial de los cambios	Autorización de cambios	Comunicar los cambios a las partes interesadas	Pruebas y aceptación de pruebas para los cambios	Implementación de cambios
Consideraciones de emergencia y contingencia	Mantener registros de cambios	Asegurar documentación operativa	Garantizar que se cambien los planes de continuidad de las TIC	Garantizar que se cambien los procedimientos de respuesta y recuperación

Proceso de Desarrollo Seguro

- Incorporar seguridad y privacidad por diseño en el ciclo completo de desarrollo.
- Reducir defectos y vulnerabilidades antes de la puesta en producción.
- Garantizar una cadena de suministro de software confiable, incluyendo dependencias y librerías.
- Estandarizar prácticas de desarrollo y revisión de código seguras.
- Integrarse con gestión de vulnerabilidades, pentesting, incidentes y cambios.
- Asegurar trazabilidad del requisito → código → prueba → despliegue.

Etapa	Descripción	Resultado esperado	Evidencias verificables
1. Requisitos y Diseño Seguro	Identificar requisitos de seguridad y privacidad desde el inicio.	Modelo de amenazas + requisitos documentados.	Diagrama de arquitectura, STRIDE, LINDDUN, requisitos en backlog.
2. Desarrollo con Estándares Seguros	Aplicar guías de codificación segura y prácticas de revisión continua.	Código consistente y con menor superficie de ataque.	Uso de estándares (OWASP / CERT), commits con convenciones, educación de desarrolladores.
3. Análisis Estático (SAST) y Dependencias (SCA)	Validación automática del código y sus librerías.	Vulnerabilidades detectadas temprano.	Reportes SAST, análisis de dependencias (SCA), alertas de versión.
4. Análisis Dinámico (DAST) y Pruebas de Seguridad	Validación de comportamiento en ejecución.	Aplicación validada bajo condiciones reales.	Reportes DAST, fuzzing, revisión de autenticación/autorización.
5. Pre-Producción y Hardening de Entorno	Validar configuración, secretos, CI/CD y contenedores.	Entorno seguro antes del despliegue.	Evidencias de IaC, escaneo de contenedores, control de secretos, checklists de despliegue.
6. Monitoreo y Respuesta en Operación	Detectar anomalías y fallos de seguridad en tiempo real.	Respuesta anticipada ante vulneración.	Logs, métricas de integridad, alertas SIEM, registros de incidentes.

Controles

Control	Nombre del Control	Tipo de Controles	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
8,25	Política de desarrollo seguro	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección
8,26	Requerimientos de seguridad en aplicaciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección #Defensa
8,27	Principios de ingeniería de sistemas seguros	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección
8,28	Codificación Segura	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección
8,29	Pruebas de seguridad en el desarrollo y aceptación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Seguridad_del_sistema_y_red #Seguridad_aplicación #Seguridad_de_información	#Protección
8,30	Restricción del acceso a la información	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Seguridad_del_sistema_y_red #Seguridad_aplicación #Relaciones_con_los_proveedores	#Gobernanza_ y_Ecosistema#Protección
8,31	Separación de ambientes de desarrollo, prueba y producción	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección
8,32	Gestión del cambio	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección
8,33	Protección de los datos de prueba	#Preventivo	#Confidencialidad #Integridad	#Proteger	#Información_protección	#Protección

8.25 Ciclo de Vida de Desarrollo de Software

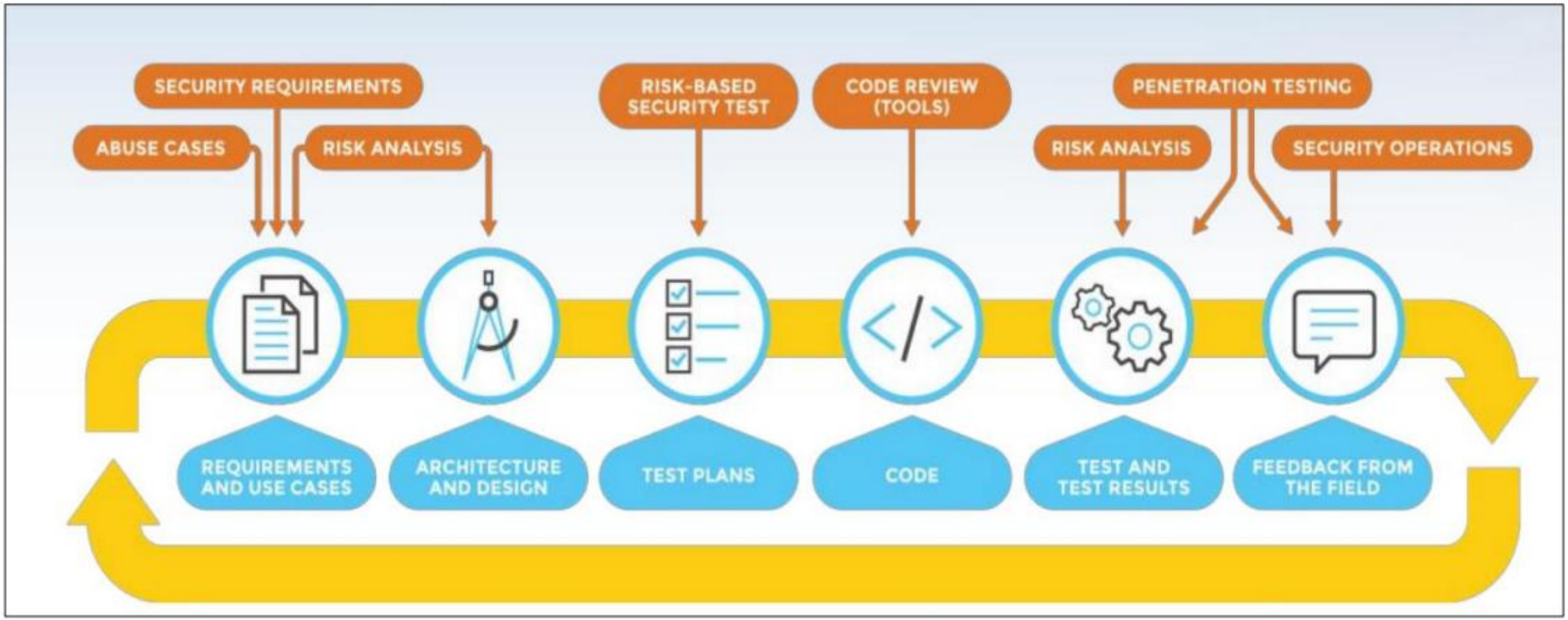
¿DEFINIR LA POLITICA?

No lo plantea explícitamente, pero es la mejor forma de abordar el control

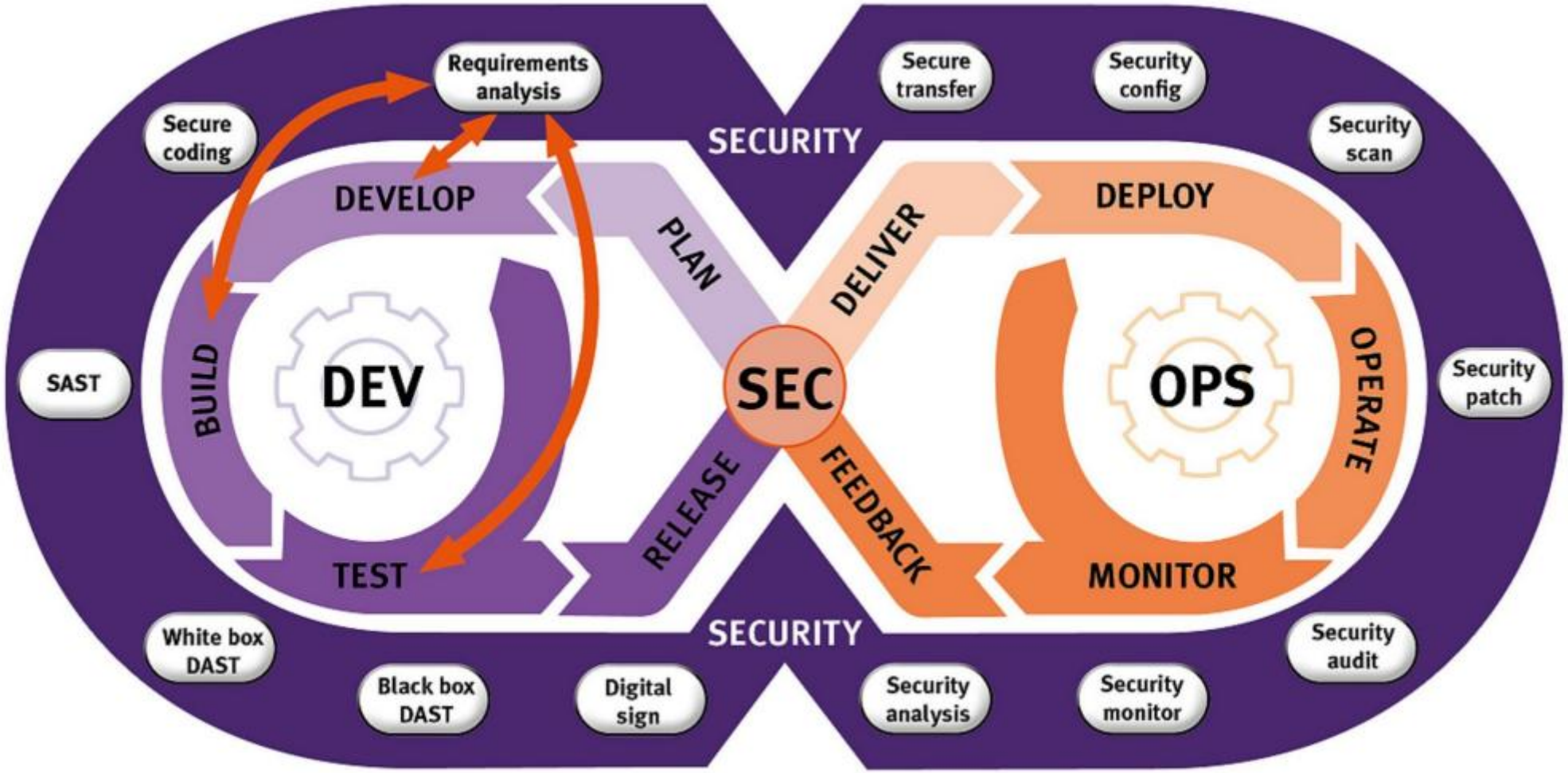
En este contexto

Separación de ambientes	(8.31)
Seguridad en la Metodología	(8.27, 8.28)
Codificación segura	(5.8)
Seguridad en el diseño	(5.8)
Seguridad en proyectos	(5.8)
Testeo de Seguridad	(8.29)
Repositorios seguros	(8.4, 8.9)
Seguridad en control de versiones	(8.32)
Entrenamiento	(8.28)
Capacidades en Vulnerabilidades	(8.28)

S-SDLC – Seguridad en el Ciclo de Vida de Desarrollo de Software



DevSecOps – Seguridad en DevOps



8.26 Requerimientos de seguridad en aplicaciones

- Generales
- Transaccionales
- Payment

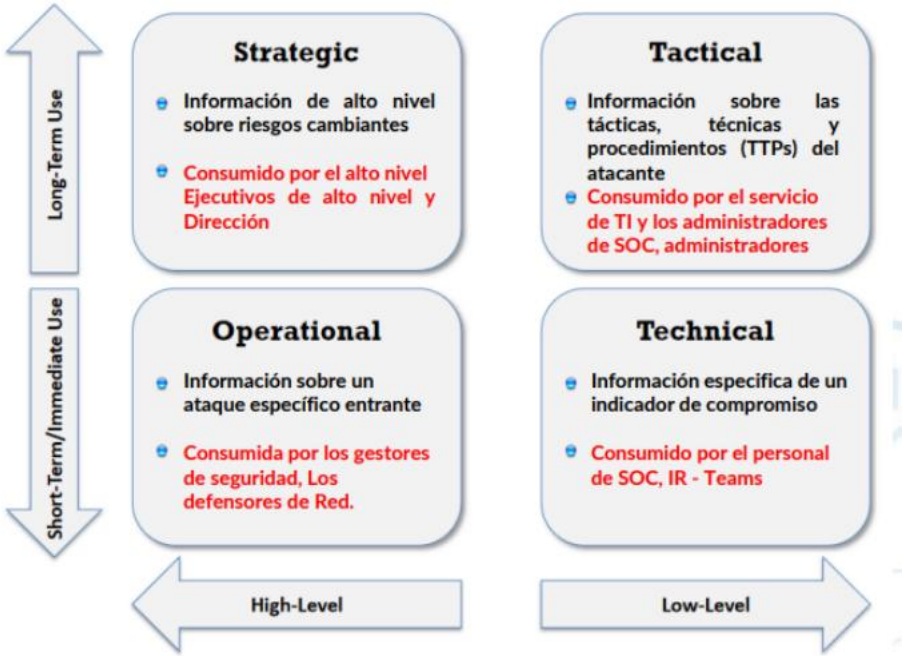
Nivel de confianza (autenticación)	Clasificación de información	Segregación de datos y funciones	Resiliencia a ataques	Requerimientos legales
Privacidad	Requisitos de confidencialidad	Protección de datos	Cifrado de comunicaciones	Controles de aplicación
Gestión de errores	Nivel de confianza de las partes	Nivel de integridad en el intercambio y procesamiento	Proceso de autorización	Intercambio de claves
Confidencialidad y requisitos de tiempo	Seguros	Confidencialidad e integridad	Seguridad en transacciones	Entorno seguro
		Seguridad con entidades de confianza		

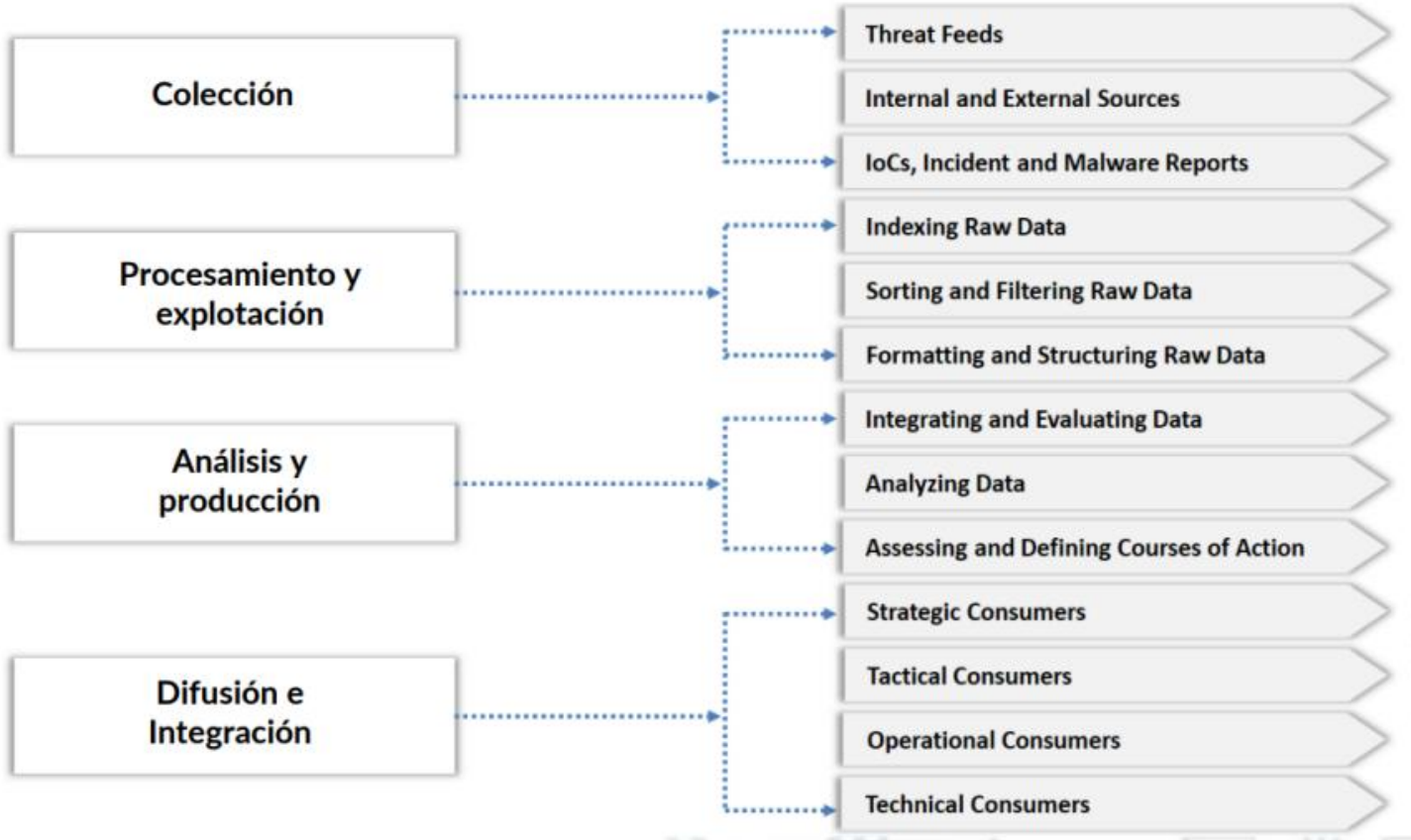
Proceso de Ciberinteligencia

- Identificar amenazas relevantes para la organización (no amenazas genéricas).
- Convertir datos técnicos (logs, IOCs, tácticas) en información útil para la toma de decisiones.
- Fortalecer la detección temprana y respuesta proactiva ante incidentes.
- Ajustar priorización de vulnerabilidades según riesgo real vs. impacto.
- Compartir inteligencia con áreas internas y, cuando corresponde, con entes nacionales (CSIRT/ANCI).
- Elevar madurez desde "reaccionar a alertas" → "anticipar campañas y patrones de ataque"

Etapa	Descripción	Resultado esperado	Evidencias verificables
1. Identificación de Necesidades de Inteligencia (IRs - Requirements)	Definir qué debemos saber y para qué (sectores, activos críticos, amenazas relevantes).	Documento de Requerimientos de Inteligencia.	Lista de activos críticos, mapa de amenazas relevantes, criterios de priorización.
2. Recolección de Información	Reunir datos desde fuentes confiables (internas, externas, OSINT, CERT/CSIRT, proveedores).	Feeds de amenazas + datos estructurados.	Suscripciones, integraciones SIEM/EDR, bitácoras de feeds, evidencia de origen.
3. Análisis y Correlación	Transformar datos en información útil: identificar campañas, patrones, TTPs.	Informes de análisis de inteligencia.	Matrices **MITRE ATT&CK**, resúmenes tácticos, análisis de indicadores (IOC/IOA).
4. Producción y Difusión	Generar reportes para audiencias (ejecutivos, SOC, incident response, vulnerabilidades).	Productos de inteligencia (táctica / operacional / estratégica).	Boletines, alertas internas, dashboards, presentaciones.
5. Aplicación en Controles y Respuesta	Ajustar configuraciones, priorizaciones y planes de respuesta.	Controles actualizados según inteligencia.	Reglas de firewall/EDR actualizadas, Playbooks IR ajustados, CVEs re-priorizados.
6. Retroalimentación y Mejora Continua	Medir si la inteligencia generó impacto real.	Métricas de efectividad de CTI.	Indicadores: MTTD ↓, falsos positivos ↓, alertas validadas ↑, incidentes evitados.

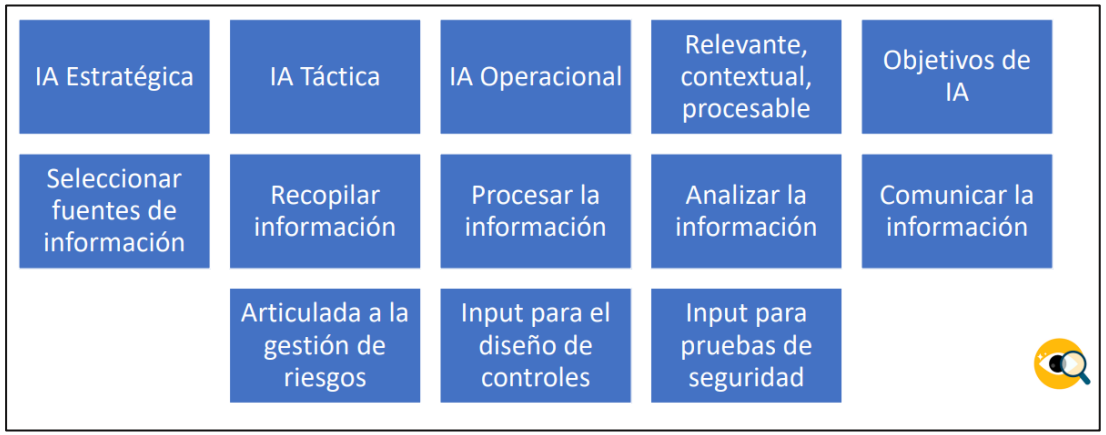
Proceso de Ciberinteligencia





Proceso de Ciberinteligencia

Marco	Control / Sección	Qué exige
ISO 27002:2022	**5.7 – Threat Intelligence**	Establecer, usar y mantener inteligencia para adaptar protección.
ISO 27001:2022	Relacionado a A.5 (Contexto, amenazas y riesgos)	La inteligencia alimenta análisis de riesgo y eficacia de controles.
CIS Controls v8.1	**Control 13 – Network Monitoring and Defense**	La inteligencia se integra en detección y reglas de SOC.
NIST SP 800-53 r5	**RA-10 – Threat Hunting / SI-4 – Monitoring / PM-12**	Detección proactiva basada en comportamiento adversario.
MITRE ATT&CK	Matriz de TTPs por actor/industria	Base para análisis táctico y playbooks de respuesta.
COBIT 2019	**DSS05 – Gestión de Seguridad de Servicios**	Inteligencia como insumo para decisiones operacionales.

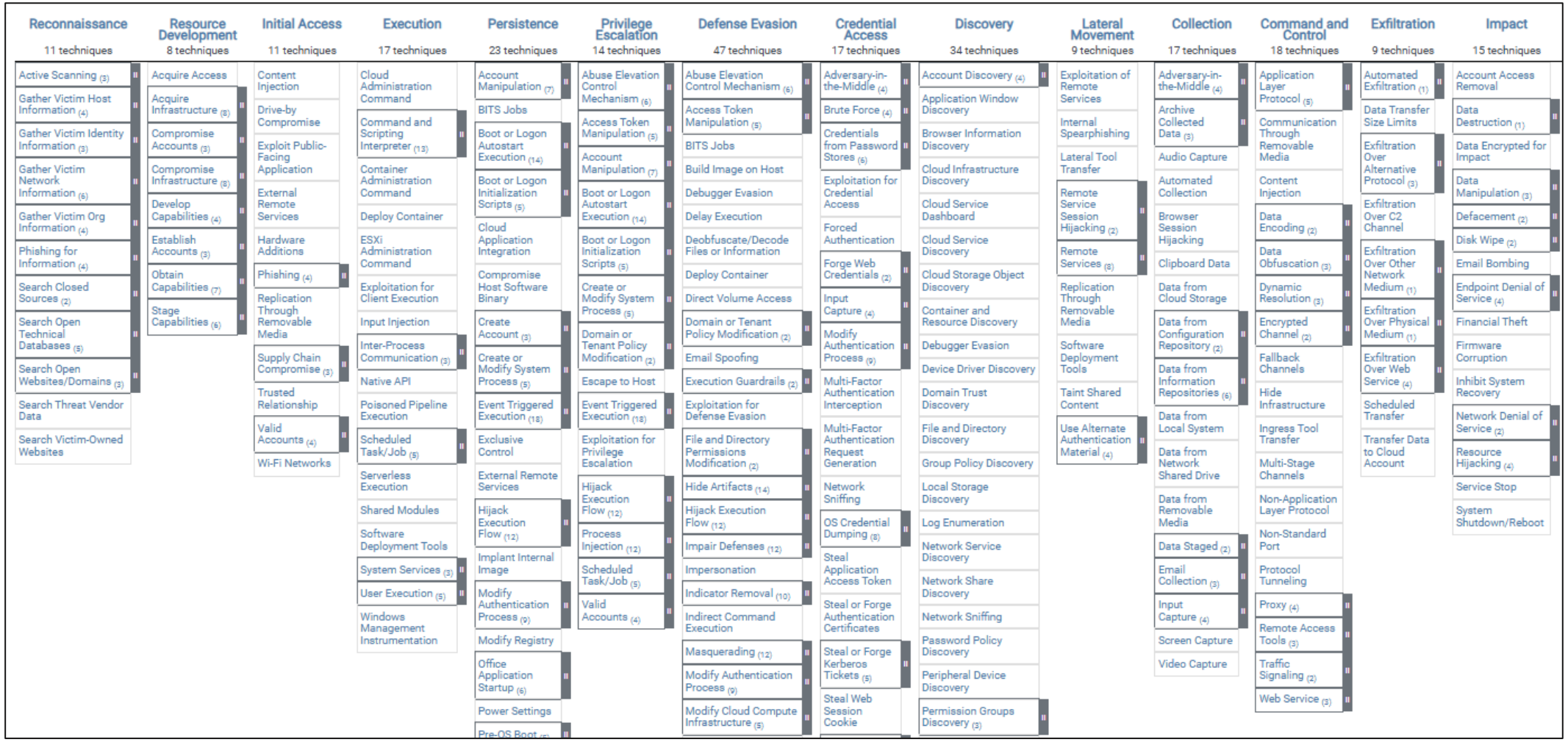


Proceso de Pentesting

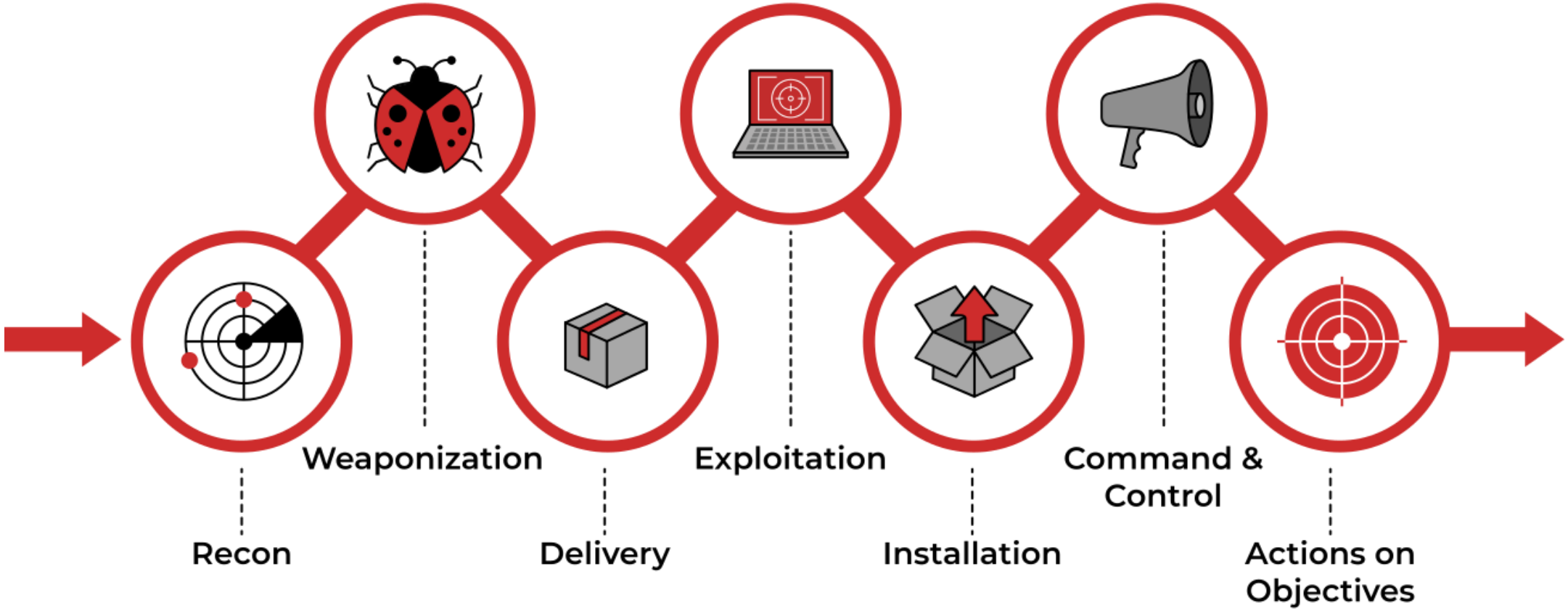
- Identificar vulnerabilidades explotables en la práctica, no solo teóricas.
- Evaluar la resiliencia de sistemas, aplicaciones, redes y servicios ante técnicas reales de ataque.
- Validar la efectividad de controles preventivos, detectivos y de respuesta.
- Priorizar correcciones según impacto real y probabilidad de explotación.
- Mejorar continuamente el modelo de seguridad con base en lecciones aprendidas del entorno ofensivo.
- Generar evidencia trazable para auditorías, cumplimiento y revisiones gerenciales.

Etapa	Descripción	Resultado esperado	Evidencias verificables
1. Planeación y Alcance (ROE)	Se definen objetivos, activos, permisos, ventanas, no-go y reglas de compromiso.	Documento de alcance y **Reglas de Enganche (ROE)** aprobadas.	Acta de alcance, matriz de activos incluidos, autorizaciones formales.
2. Reconocimiento y Enumeración	Identificación de vectores, superficies de ataque, servicios y tecnologías.	Mapa de superficie de ataque.	Evidencia de escaneos, OSINT, fingerprinting, diagramas.
3. Explotación Controlada	Intentos de explotación para validar impacto real.	Evidencia del riesgo **con prueba controlada**.	Capturas, PoC, logs, registros de explotación con autorización.
4. Escalada y Movimiento Lateral (si aplica)	Validación de impacto sistémico.	Determinación clara del **riesgo mayor**.	Matriz MITRE ATT&CK, trazabilidad de pasos y privilegios obtenidos.
5. Reporte Ejecutivo y Técnico	Integración de resultados y recomendaciones priorizadas.	Informe en dos niveles (estratégico y técnico).	Informe con hallazgos, criticidad (CVSS + contexto), recomendaciones.
6. Remediación y Re-Test	Validación de correcciones aplicadas.	Confirmación de que la vulnerabilidad fue cerrada.	Evidencia comparativa pre/post, re-test firmado, cierre documentado.

Proceso de Pentesting – Visión Mitre



Proceso de Pentesting – Cyber Kill Chain



Proceso de Monitoreo de Red y Servicios

- Supervisar en tiempo real la operación de redes, sistemas y servicios críticos para detectar anomalías y fallas.
- Detectar comportamientos sospechosos o maliciosos antes de que se materialicen incidentes.
- Integrar información de múltiples fuentes (logs, telemetría, sensores, flujos de red) para obtener visibilidad unificada.
- Permitir una respuesta temprana, reduciendo impacto y ventana de exposición
- .Generar alertas accionables, no ruido ni falsas alarmas.
- Alimentar decisiones de mejora continua, hardening y protección adaptativa.

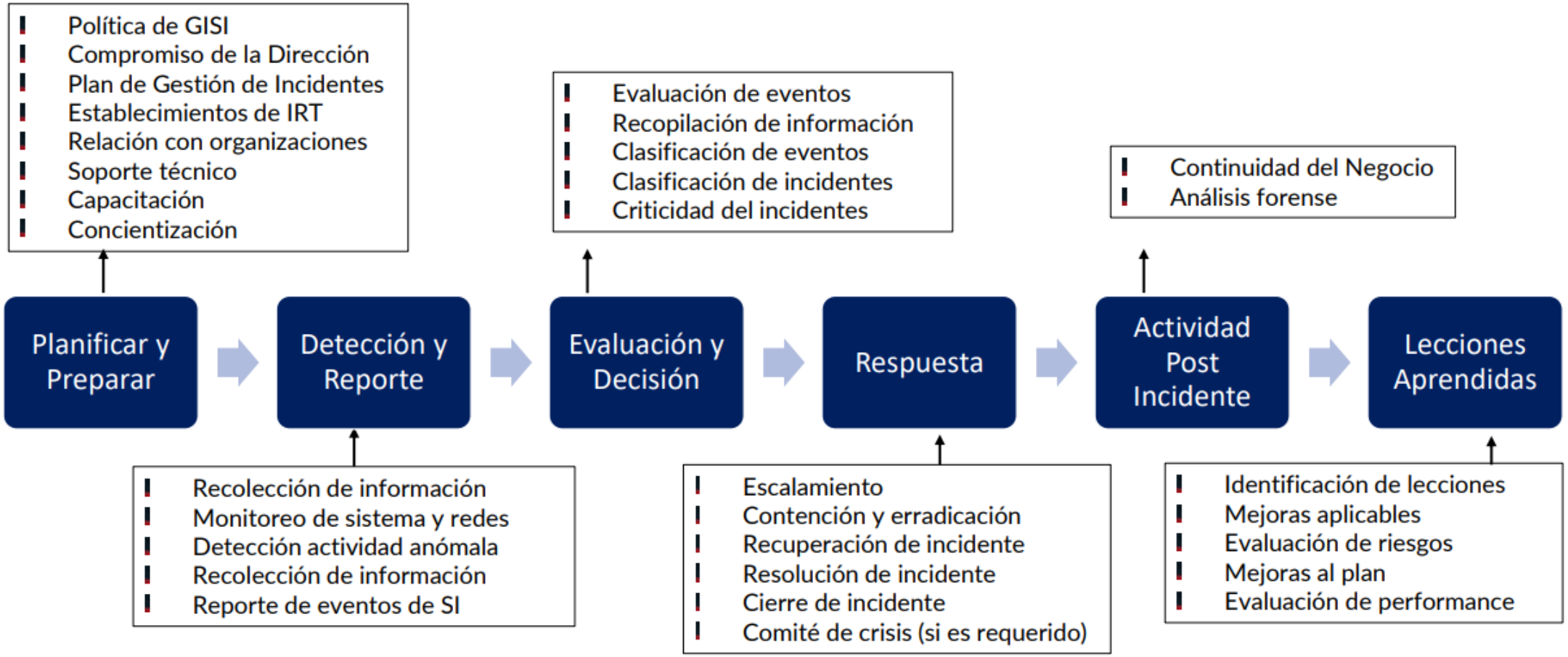
Etapa	Descripción	Resultado esperado	Evidencias verificables
1. Identificación de Activos y Servicios Críticos	Determinar qué debe ser monitoreado (priorización).	Mapa de monitoreo basado en criticidad.	Inventario de activos + CMDB + topología de red + lista de servicios críticos.
2. Recolección y Normalización de Datos	Obtener logs, métricas, flujos, telemetría, EDR/XDR, NetFlow.	Datos estructurados en plataforma central.	Configuración SIEM, syslog, agentes EDR, tablas de correlación.
3. Definición de Umbrales y Reglas de Detección	Establecer eventos relevantes y criterios de alerta.	Reglas de alerta significativas y priorizadas.	Manual de casos de uso, reglas en SIEM/IDS, dashboards.
4. Monitoreo Continuo y Correlación	Detección en tiempo real de anomalías o actividad maliciosa.	Alertas con severidad y contexto.	Consola SOC, tickets registrados, trazabilidad de alertas.
5. Notificación y Escalamiento	Alertas accionables según matriz de escalamiento.	Comunicación clara con equipos de respuesta.	Registro de alertas, tiempos de reacción (MTTD/MTTR), evidencias de escalamiento.
6. Retroalimentación y Mejora Continua	Ajuste de reglas y cobertura según incidentes reales.	Monitoreo más fino, menos falsos positivos.	Historial de tuning, revisión mensual con SOC/seguridad.

Proceso de Gestión de Incidentes

- Detectar y responder rápidamente a incidentes de seguridad para minimizar impacto.
- Coordinar equipos técnicos, negocio, proveedores y autoridades cuando corresponde.
- Preservar evidencia para investigación y cumplimiento regulatorio.
- Restablecer continuidad de servicios afectados de manera controlada.
- Comunicar oportunamente a stakeholders clave (internos/externos).
- Generar lecciones aprendidas que alimenten mejora del SGSI y controles preventivos.

Etapa	Descripción	Resultado esperado	Evidencias verificables
1. Preparación	Definir roles, contactos, herramientas, playbooks y capacidades.	Plan de Respuesta a Incidentes (PRI) vigente.	Procedimiento IR, contactos, plantillas, entrenamiento, simulaciones.
2. Detección y Análisis	Identificación de anomalías o señales de compromiso.	Ticket de incidente con clasificación inicial.	Alertas SIEM/EDR, análisis de logs, correlación MITRE ATT&CK.
3. Contención Inicial	Limitar el alcance y evitar propagación o daño mayor.	Incidente aislado y contenido.	Evidencia de bloqueo, desactivación, microsegmentación, snapshots.
4. Erradicación y Remediación	Eliminar la causa raíz y restaurar configuraciones seguras.	Riesgo eliminado o mitigado.	Reportes de remediación, parches aplicados, reposición de configuraciones.
5. Recuperación	Restablecer servicio en forma **controlada y validada**.	Servicio restablecido sin reinfección.	Bitácoras de recuperación, validación post-restauración, pruebas de integridad.
6. Lecciones Aprendidas y Cierre	Mejorar procesos y controles basados en el incidente.	Informe final + acciones de mejora.	Analisis forense, RCA (Root Cause Analysis), actualización de playbooks y controles.

Proceso de Gestión de Incidentes – Desde ISO 27035



5.24 Planificación y preparación (ISO 27002)

Roles y Responsabilidades

- Método común de reporte
- Proceso de Gestión de Incidentes
- Proceso de Respuesta a Incidentes
- Competencia Profesional
- Identificar training requerido

Procedimientos

- Evaluación de Eventos
- Detección y análisis de eventos e incidentes
- Escalamiento y Respuesta
- Manejo de Evidencia
- Análisis de la causa
- Lecciones Aprendidas

Procedimiento de Reporte

- Acciones frente a un evento
- Uso de Formularios
- Proceso de retroalimentación
- Creación de informes de incidentes

Proceso de Gestión de Incidentes – Desde COBIT 2019

B. Componente: Estructuras organizativas						
Práctica clave de gestión	Director de tecnología	RDueños del proceso de negocio	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de la información
DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.	A		R	R	R	
DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.	A			R	R	
DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	A	R	R	R	R	
DSS02.04 Investigar, diagnosticar y asignar incidentes.	A	R		R	R	
DSS02.05 Resolver y recuperarse de los incidentes.	A		R	R	R	R
DSS02.06 Cerrar las peticiones de servicio y los incidentes.	A			R	R	R
DSS02.07 Hacer seguimiento al estado y producir informes.	A			R	R	

Resumen de Controles de Gestión de Incidentes – ISO 27002

Control	Nombre del Control	Tipo de Controles	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
5,24	Responsabilidades y procedimientos	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Información_seguridad_gestión_de_eventos	#Defensa
5,25	Evaluación y decisión sobre los eventos de seguridad de información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Información_seguridad_gestión_de_eventos	#Defensa
5,26	Respuesta a incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Información_seguridad_gestión_de_eventos	#Defensa
5,27	Aprendizaje de los incidentes de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Identificar	#Información_seguridad_gestión_de_eventos	#Defensa
5,28	Recopilación de evidencias	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Información_seguridad_gestión_de_eventos	#Defensa
6,80	Reporte de eventos de seguridad de la información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Información_seguridad_gestión_de_eventos	#Defensa

Resumen de Controles de Gestión de Incidentes – ISO 27002

Marco	Sección / Control	Qué exige
ISO 27001:2022	A.5.25–A.5.28	Preparación, detección, respuesta, mejoras.
ISO 27002:2022	**8.16, 8.18, 8.19, 8.20**	Gestión de logs, monitoreo, clasificación y respuesta.
ISO 27035 (1/2/3)	**Norma específica para gestión de incidentes**	Proceso completo y guías operativas.
NIST SP 800-61r2	*Computer Security Incident Handling Guide*	Framework IR más usado globalmente.
CIS Controls v8.1	Control 17 – IR & Testing	Equipos, playbooks, entrenamiento y simulaciones.
MITRE ATT&CK	Base para análisis de TTPs	Entender el comportamiento del adversario.

Ley	Exigencia
Ley Marco de Ciberseguridad	*Notificación de incidentes significativos a CSIRT/ANCI*
Ley 21.719 (Protección de Datos)	Notificar **brechas de datos personales** según severidad

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Visión de Procesos de Ciberseguridad

Workshop N°1

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD