Control Anexo A	Grupo	Nombre	Descripción	Aplicación/Excluído	Tipo de control	Información (propiedades seguridad)	Conceptos	Operacional Capacidades	Dominios de Seguridad	Justificación	Gestión
A.5.1	Controles organizacionales	Políticas para la seguridad de la información	Control La política de seguridad de la información y un conjunto de políticas temáticas específicas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Gobernanza	Gobernanza y ecosistema Protección Resiliencia	Las políticas permiten regular el comportamiento de los trabajadores en cuanto a la seguridad de la información	Existen políticas de seguridad aprobadadas y adecuadas a nuestras necesidades. Las políticas se ponen a disposición de todo el personal en el sistema de gestión. Se realizan campañas de comunicación Las políticas tienen definida una frecuencia de revisión gestionada por el propio sistema. Los cambios en las políticas se comunican desde el correo del comité de riesgos
A.5.2	Controles organizacionales	Roles y responsabilidades en seguridad de la información	Control Todos los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Gobernanza	Gobernanza y ecosistema Protección Resiliencia	Conocer los roles y responsabilidades de seguridad permite dar respuesta oportuna y eficaz del equipo de trabajo	Las responsabilidades de seguridad de la información están definidas en los perfiles de puesto de trabajo y complementadas mediante una matriz RACI, que establece claramente los roles responsables, aprobadores, consultados e informados para las actividades y procesos relevantes.
A.5.3	Controles organizacionales	Segregación de tareas	Las funciones y áreas de responsabilidad en conflicto deben segregarse.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gobernanza	Gobernanza y ecosistema Protección	Las funciones en conflicto (autorización/aprobación vs ejecución) pueden generar riesgos de fraude o error en procesos críticos. Se aplica el control para segregar responsabilidades según análisis de riesgos del SGI.	Se documentan roles y responsabilidades que segregan funciones conflictivas: autorización de accesos y cambios corresponde a responsable técnico, mientras ejecución operativa sigue principio de mínimo privilegio. Se complementa con registros auditables de operaciones críticas y aprobaciones dobles en procesos sensibles, asegurando controles y equilibrios organizativos.
A.5.4	Controles organizacionales	Responsabilidades de la dirección	Control La dirección debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información, las políticas temáticas y sus procedimientos específicos establecidos en la organización.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Gobernanza	Gobernanza y ecosistema Protección	La dirección tiene la responsabilidad última de garantizar la aplicación efectiva de la seguridad de la información en toda la organización. Se aplica el control para exigir al personal el cumplimiento de la política de seguridad de la información, políticas temáticas y procedimientos específicos del SGI.	La dirección demuestra compromiso visible mediante aprobación de la política de seguridad de la información, asignación de recursos necesarios y participación en revisiones de dirección periódicas del SGI. Se comunica explícitamente a todo el personal la obligación de cumplir las políticas y procedimientos de seguridad en incorporación y contratos laborales.
A.5.5	Controles organizacionales	Contacto con las autoridades	Control Deben establecerse y mantenerse los contactos adecuados con las autoridades pertinentes.	Aplica	Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Identificar Proteger Responder Recuperar	Gobernanza	Defensa Resiliencia	Los incidentes graves de seguridad pueden requerir notificación o colaboración con autoridades competentes según legislación española. Se aplica el control para mantener contactos adecuados con autoridades pertinentes, asegurando respuesta coordinada ante eventos significativos del SGI.	Se identifican y mantienen contactos actualizados con autoridades clave: INCIBE (ciberincidentes), Agencia Española de Protección de Datos (AEPD) y cuerpos policiales locales. Los procedimientos de gestión de incidentes incluyen criterios de notificación obligatoria/voluntaria y canales de comunicación establecidos. El responsable de seguridad coordina cualquier contacto oficial.
A.5.6	Controles organizacionales	Contacto con grupos de interés especial	Control Deben establecerse y mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializados en seguridad.	Aplica	Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Proteger Responder Recuperar	Gobernanza	Defensa Resiliencia	La colaboración con grupos especializados permite acceder a inteligencia de amenazas actualizada, mejores prácticas y respuesta coordinada ante incidentes sectoriales. Se aplica el control para mantener contactos apropiados con asociaciones profesionales de seguridad de la información.	Se mantienen suscripciones a grupos de profesionales y entidades relacionadas con la seguridad de la información, principalmente en el modo de suscripción a boletines o foros (por ejemplo, INCIBE).
A.5.7	Controles organizacionales	Inteligencia de amenazas	Control La información relativa a las amenazas a la seguridad de la información debe recopilarse y analizarse para producir información sobre amenazas.	Aplica	Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Identificar Detectar Responder	Amenaza y Vulnerabilidad - Gestión Habilidades	Defensa Resiliencia	Las amenazas externas evolucionan continuamente, requiriendo inteligencia actualizada para anticipar y mitigar riesgos a datos privados de negocio y empleados. Se aplica el control para recopilar y analizar información de amenazas relevantes al contexto organizativo y análisis de riesgos del SGI.	Se recopila inteligencia de amenazas mediante suscripción a boletines oficiales (INCIBE, CVE, proveedores clave) y fuentes especializadas en software/desarrollo. El responsable de seguridad analiza periódicamente información relevante, identificando amenazas aplicables y distribuyendo alertas prioritarias al equipo técnico.
A.5.8	Controles organizacionales	Seguridad de la información en la gestión de proyectos	Control La seguridad de la información debe integrarse en la gestión de proyectos.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar Proteger	Gobernanza	Gobernanza y ecosistema Protección	Los proyectos pueden introducir vulnerabilidades si la seguridad no se considera desde su concepción. Se aplica el control para integrar requisitos de seguridad de la información en la gestión de proyectos.	Se describe en el procedimiento de Seguridad de la información en la gestión de proyectos cómo se aborda un análisis de riegos en los proyectos de la compañía relacionados con el sistema de gestión.
A.5.9	Controles organizacionales	Inventario de información y otros activos asociados	Control Debe elaborarse y mantenerse un inventario de la información y otros activos asociados, incluyendo la identificación de sus propietarios.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Gestion de Activos	Gobernanza y ecosistema Protección	El inventario de activos es esencial para identificar, clasificar y asignar responsabilidades de protección a toda la información privada de negocio, datos de empleados y recursos asociados (hardware, software, servicios). Se aplica el control para mantener control efectivo sobre todos los elementos del SGI según análisis de riesgos.	Se mantiene un inventario actualizado de activos de la empresa. El inventario de activos ayuda a asegurar una protección eficaz de la información.
A.5.10	Controles organizacionales	Uso aceptable de la información y activos asociados	Control Se deben identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de información y otros activos asociados.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gestión de Activos Protección de Datos	Gobernanza y ecosistema Protección	El uso inadecuado de información privada de negocio, datos de empleados y activos tecnológicos puede generar fugas, interrupciones o exposición a malware. Se aplica el control para identificar, documentar e implementar reglas de uso aceptable y procedimientos de manejo, según análisis de riesgos	Se documenta y comunica política de uso aceptable que define reglas para el manejo de información clasificada, dispositivos corporativos, redes, software autorizado y teletrabajo. La política se revisa anualmente y se acepta por los empleados en el onboarding o ante cambios significativos.
A.5.11	Controles organizacionales	Devolución de activos	Control Todos los empleados y otras terceras partes, según procedan, deben devolver todos los activos de la organización en su poder tras el cambio o la terminación de su trabajo, contrato o acuerdo.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gestion de Activos	Protección	La no devolución de activos (hardware, accesos, datos) tras terminación laboral o contractual genera riesgos de fugas de información sensible, accesos no autorizados o pérdida material. Se aplica el control para exigir la devolución formal de todos los activos según inventario, alineado con análisis de riesgos	A la finalización de la relación contractual con un empleado, La dirección solicita la devolución de los activos, utilizando el inventario y firmando una hoja de devolución
A.5.12	Controles organizacionales	Clasificación de la información	Control La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Protección de Datos	Protección Defensa	La información clasificada (código fuente, datos clientes, documentación contratos) requiere protección diferenciada según confidencialidad, integridad, disponibilidad y requisitos de partes interesadas.	Se establece una clasificación por niveles según la sensibilidad. La clasificación de los activos se define en el PROC. Clasificación de la información y en la POL. Clasificación de la información
A.5.13	Controles organizacionales	Etiquetado de la información	Control Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Protección de Datos	Protección Defensa	Sin etiquetado, los controles de manejo no se aplican correctamente, generando riesgos de divulgación accidental. Se aplica para implementar procedimientos de etiquetado según esquema de clasificación.	El procedimiento de etiquetado queda descrito en el procedimiento y registrado en el inventario de activos
A.5.14	Controles organizacionales	Transferencia de la información	Control Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de medios de transferencia dentro de la organización y entre la organización y otras partes.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gestión de Activos Protección de Datos	Protección	Se cree necesario el establecimiento de normas que rijan el intercambio de información en la organización, ya que esta es una actividad que puede afectar gravemente la seguridad de la información si no se lleva a cabo adecuadamente	Se define un marco de trabajo seguro para la transferencia de información, tanto interna como externa, protegiendo la confidencialidad, integridad y disponibilidad de los datos.
A.5.15	Controles organizacionales	Control de acceso	Control Se deben establecer e implementar reglas de control de acceso físico y lógico a la información y otros activos asociados, basadas en los requisitos de negocio y de seguridad de la información.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y Gestión Acceso	Protección	Controlar los accesos propicia que los perfiles correspondientes tengan acceso correcto a los activos de información que le corresponden y evite que personas no autorizadas accedan a información que no les corresponde.	Mediante el procedimiento de control de accesos, de política de seguridad física. y Politica de Seguridad en la Identificacion y autentificacion el responsable de Seguridad se encarga de realizar las altas y bajas de usuarios.

Control Anexo A	Grupo	Nombre	Descripción	Aplicación/Excluído	Tipo de control	Información (propiedades seguridad)	Conceptos	Operacional Capacidades	Dominios de Seguridad	Justificación	Gestión
A.5.16	Controles organizacionales	Gestión de identidad	Control Se debe gestionar el ciclo de vida completo de las identidades.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y Gestión Acceso	Protección	Identidades no gestionadas generan accesos huérfanos, escalada de privilegios y riesgos insider threats críticos en repositorios código, servidores y datos clientes. Se aplica para gestionar ciclo completo (creación, modificación, desactivación) de identidades, alineado con inventario activos, clasificación información y terminaciones.	Se han definido formalmente las reglas para el alta y baja de los usuarios en PROC. Gestión de identidad
A.5.17	Controles organizacionales	Información de autenticación	Control La asignación y gestión de la información de autenticación debe controlarse mediante un proceso formal de gestión, incluyendo el asesoramiento al personal sobre el tratamiento adecuado de la información de autenticación.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y Gestión Acceso	Protección	Credenciales mal gestionadas representan vector principal de compromiso en repositorios y servidores. Se aplica para controlar asignación y manejo formal de información de autenticación, alineado con gestión identidades, privilegios y análisis riesgos SGI.	Cada usuario dispone de credenciales individuales para los sistemas a los que tiene acceso, aplicándose controles para evitar la suplantación de identidad. La información de autenticación se gestiona mediante un proceso formal y, cuando resulta necesario, se almacena y administra utilizando un gestor de contraseñas corporativo. Se proporciona concienciación al personal sobre la creación, uso, custodia y confidencialidad de sus credenciales, así como sobre la prohibición de compartirlas.
A.5.18	Controles organizacionales	Derechos de acceso	Control Los derechos de acceso a la información y otros activos asociados deben aprovisionarse, revisarse, modificarse y eliminarse de conformidad con la política específica de la organización y las reglas sobre control de acceso.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y Gestión Acceso	Protección	Garantizar el acceso a los usuarios autorizados e impedir el acceso no autorizado a los sistemas de información	Se han definido formalmente las reglas para el alta y baja de los usuarios. La gestión se realiza según lo descrito en el PROC. Gestión y control de acceso.
A.5.19	Controles organizacionales	Seguridad de la información en las relaciones con los proveedores	Control Se deben identificar e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios de proveedores.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Relación Proveedores Seguridad	Gobernanza y ecosistema Protección	Proveedores cloud alojan infraestructura crítica que soporta código fuente, datos, operaciones desarrollo, introduciendo riesgos de disponibilidad, integridad y cumplimiento regulatorio (DORA). Se aplica para identificar/implementar procesos gestión riesgos.	Se dispone de una política de seguridad con proveedores y de procedimientos para la selección, seguimiento y control de proveedores
A.5.20	Controles organizacionales	Abordar la seguridad de la información dentro de los acuerdos de proveedores	Control Deben establecerse y acordarse con cada proveedor los requisitos pertinentes de seguridad de la información en función del tipo de relación con el proveedor.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Relación Proveedores Seguridad	Gobernanza y ecosistema Protección	Los proveedores pueden alojar infraestructura crítica que soporta operaciones desarrollo, introduciendo riesgos de confidencialidad, disponibilidad y cumplimiento regulatorio (DORA). Se aplica para establecer requisitos específicos de seguridad en contratos proveedores.	Se incluyen cláusulas de seguridad ISO27001, resiliencia, auditoría y notificación incidentes en contratos. Existen procedimientos revisión contractual anual para validar cumplimiento requisitos acordados.
A.5.21	Controles organizacionales	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Control Se deben definir e implementar procesos y procedimientos para hacer frente a los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de Tecnologías de la Información y de las Comunicaciones (TIC).	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Relación Proveedores Seguridad	Gobernanza y ecosistema Protección	Proveedores TIC (cloud, licencias software, herramientas desarrollo) forman cadena suministro crítica que soporta operaciones, introduciendo riesgos de vulnerabilidades componentes, configuraciones inseguras y cumplimiento regulatorio (DORA). Se aplica para definir procesos gestión riesgos cadena suministro TIC	Para evitar que la contratación de un proveedor introduzca posibles vulnerabilidades, se toman diversas medidas de seguridad, según recoge la documentación sobre la relación con proveedores.
A.5.22	Controles organizacionales	Seguimiento, revisión y gestión del cambio de los servicios de proveedores	Control La organización debe supervisar, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información y prestación de servicios de los proveedores.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Relación Proveedores Seguridad	Gobernanza y ecosistema Protección Defensa Garantía Seguridad de la Información	Proveedores cloud pueden modificar configuraciones, políticas seguridad o servicios sin notificación, afectando disponibilidad, integridad y cumplimiento DORA de infraestructura crítica desarrollo. Se aplica para supervisar regularmente cambios servicios proveedores cloud.	Revisión periódica contratos SLA cloud y cambios servicios documentados. Validación de configuraciones críticas en renovaciones contractuales y registro de cambios.
A.5.23	Controles organizacionales	Seguridad de la información para el uso de servicios en la nube	Control Los procesos de adquisición, uso, gestión y finalización de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Relación Proveedores Seguridad	Gobernanza y ecosistema Protección	Servicios cloud alojan infraestructura crítica de desarrollo software, introduciendo riesgos de configuración insegura, fugas datos y cumplimiento DORA. Se aplica para establecer procesos adquisición, uso y finalización servicios cloud alineados con requisitos SGI.	La seguridad de la información para el uso de servicios en la nube está contemplada en un procedimiento formal de la organización.
A.5.24	Controles organizacionales	Planificación y preparación de la gestión de incidentes de seguridad de información	Control La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de los procesos, roles y responsabilidades de gestión de los incidentes de seguridad de la información.	Aplica	Correctivo	Confidencialidad Integridad Disponibilidad	Responder Recuperar	Gobernanza Gestión Información y Eventos Seguridad	Defensa	La gestión de incidentes permite actuar de forma oportuna ante situaciones que pueden afectar la disponibilidad, la confidencialidad y la integridad de los activos de la información	Se dispone de un procedimiento para la gestión de incidentes de seguridad de la información, que define las etapas desde la detección o comunicación del incidente hasta su resolución y cierre, así como los roles, responsabilidades y canales de comunicación aplicables. El procedimiento se revisa periódicamente y se realizan pruebas o ejercicios de simulación para verificar su eficacia y la preparación de los responsables. Los resultados se documentan y, cuando procede, se establecen acciones de mejora.
A.5.25	Controles organizacionales	Evaluación y decisión sobre los eventos de seguridad de información	Control La organización debe evaluar los eventos de seguridad de la información y decidir si deben ser catalogados como incidentes de seguridad de la información.	Aplica	Detectivo	Confidencialidad Integridad Disponibilidad	Detectar Responder	Gestión Información y Eventos Seguridad	Defensa	Los eventos de seguridad (fallos, debilidades, anomalías) pueden escalar a incidentes si no se evalúan oportunamente, afectando disponibilidad y confidencialidad de información crítica. Se aplica para evaluar eventos y decidir catalogación como incidentes, alineado con gestión de incidentes SGI.	Las debilidades, eventos y posibles incidentes de seguridad de la información se registran en el sistema corporativo de gestión de tickets. Tras una evaluación inicial, se clasifican como probable incidente o improbable incidente, determinándose el tratamiento y la prioridad correspondientes. Los casos que proceden se escalan al procedimiento de gestión de incidentes, manteniéndose trazabilidad de su seguimiento y cierre.
A.5.26	Controles organizacionales	Respuesta a incidentes de seguridad de la información	Control Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Aplica	Correctivo	Confidencialidad Integridad Disponibilidad	Responder Recuperar	Gestión Información y Eventos Seguridad	Defensa	Los incidentes de seguridad pueden escalar rápidamente afectando disponibilidad, integridad y confidencialidad de información crítica si no se responden según procedimientos establecidos. Se aplica para garantizar respuesta oportuna y efectiva a incidentes mediante planes documentados.	Los incidentes de seguridad de la información se gestionan de acuerdo con un procedimiento documentado que establece las pautas de notificación, evaluación, escalado, contención, erradicación y recuperación, en función de su naturaleza e impacto. El procedimiento define los roles y responsabilidades implicados, así como los criterios y canales de comunicación aplicables. Una vez resuelto el incidente, se documentan las actuaciones realizadas, las conclusiones y, cuando procede, las acciones de mejora. El procedimiento se revisa al menos anualmente y siempre que se produzcan cambios relevantes o se identifiquen necesidades de actualización.
A.5.27	Controles organizacionales	Aprender de los incidentes de seguridad de la información	Control El conocimiento adquirido a partir de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar Proteger	Gestión Información y Eventos Seguridad	Defensa	El conocimiento de incidentes resueltos fortalece controles SGI evitando recurrencia y mejorando respuesta futura. Se aplica para analizar lecciones aprendidas tras incidentes y replicar soluciones efectivas en sistema gestión.	Tras la resolución de los incidentes de seguridad de la información, se analizan sus causas, el tratamiento aplicado y la eficacia de la respuesta. Cuando procede, se documentan las lecciones aprendidas y se establecen acciones de mejora para reforzar los controles y prevenir incidentes similares. La información obtenida se considera en la actualización de procedimientos y medidas de seguridad, y se revisan periódicamente los incidentes registrados para identificar tendencias.

Control Anexo A	Grupo	Nombre	Descripción	Aplicación/Excluído	Tipo de control	Información (propiedades seguridad)	Conceptos	Operacional Capacidades	Dominios de Seguridad	Justificación	Gestión
A.5.28	Controles organizacionales	Recopilación de evidencias	Control La organización debe establecer e implementar procedimientos para la identificación, recogida, adquisición y preservación de evidencias relacionadas con eventos de seguridad de la información.	Aplica	Correctivo	Confidencialidad Integridad Disponibilidad	Detectar Responder	Gestión Información y Eventos Seguridad	Defensa	Las evidencias de eventos/incidentes (logs, capturas, configuraciones) son esenciales para análisis forense, cumplimiento legal y auditorías. Se aplica para establecer procedimientos identificación, recogida y preservación evidencias de seguridad de la información.	Procedimientos documentados para recolección/protección evidencias establecidos en SGI. Equipo respuesta incidente identifica/recoge evidencias tras evento. Evidencias vinculadas a análisis de lecciones aprendidas para fortalecimiento SGI.
A.5.29	Controles organizacionales	Seguridad de la información durante la interrupción	Control La organización debe planificar cómo mantener la seguridad de la información a un nivel adecuado durante la Interrupción.	Aplica	Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Proteger Responder	Continuidad	Protección Resiliencia	Durante interrupciones (ciberataques, fallos cloud, desastres) la seguridad información puede verse comprometida si no se planifica específicamente, afectando confidencialidad y cumplimiento DORA. Se aplica para mantener controles SGSI mínimos durante situaciones de interrupción.	Los planes y procedimientos de continuidad establecen las medidas necesarias para mantener un nivel adecuado de seguridad de la información durante situaciones de interrupción. Se contemplan medidas de protección de la información, control de accesos, comunicación segura y recuperación priorizada de los servicios críticos. Una vez restablecidos los servicios, se realizan las comprobaciones necesarias para verificar su correcto funcionamiento y la integridad de la información.
A.5.30	Controles organizacionales	Preparación para las TIC para la continuidad del negocio	Control La resiliencia de las TIC debe planificarse, implantarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	Aplica	Correctivo	Disponibilidad	Responder	Continuidad	Resiliencia	Las TIC soportan operaciones críticas de desarrollo y alojan información sensible en cloud, requiriendo resiliencia planificada para cumplir objetivos continuidad negocio y DORA. Se aplica para planificar, implantar, mantener y probar resiliencia TIC alineada con BIA del SGI.	La resiliencia de las TIC se gestiona conforme a los objetivos de continuidad del negocio y los requisitos de continuidad tecnológica, tomando como referencia el BIA y el RIA. Se analizan e implantan estrategias y soluciones de continuidad para los procesos y servicios críticos, considerando sus dependencias y objetivos de recuperación. Estas soluciones se mantienen y prueban periódicamente para verificar su eficacia y detectar oportunidades de mejora.
A.5.31	Controles organizacionales	Identificación de requisitos legales, reglamentarios y contractuales	Control Los requisitos legales, estatuarios, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben ser identificados, documentados y mantenerse actualizados.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Legal y Cumplimiento	Gobernanza y ecosistema Protección	La organización debe cumplir requisitos legales, estatutarios y contractuales (RGPD, DORA, LOPD, ENS) aplicables a todos los procesos de la organización.	Se dispone de un procedimiento de Cumplimiento, que identifica, actualiza y registra los requisitos legales, normativos, contractuales y de otra índole relacionados con la seguridad de la información, con el objeto de evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a esta materia o de los requisitos de seguridad aplicables.
A.5.32	Controles organizacionales	Derechos de propiedad intelectual (DPI)	Control La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual (DPI).	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Legal y Cumplimiento	Gobernanza y ecosistema Protección	Código fuente propio, metodologías desarrollo y documentación técnica representan activos DPI críticos que requieren protección contra divulgación no autorizada o uso indebido. Se aplica para implementar procedimientos protección derechos propiedad intelectual de la organización.	Se dispone de una política de derechos de propiedad intelectual que establece las normas para el uso, protección y custodia del código fuente propietario, la documentación técnica, las metodologías internas y demás activos protegidos. Los procedimientos aplicables incluyen acuerdos de confidencialidad con empleados, colaboradores y contratistas, controles de acceso a los repositorios y restricciones sobre la copia, divulgación, modificación y uso no autorizado de dichos activos. Asimismo, se consideran los requisitos legales, contractuales y de licencia aplicables, y se realizan revisiones periódicas para verificar el cumplimiento de estas medidas.
A.5.33	Controles organizacionales	Protección de los registros	Control Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar Proteger	Legal y Cumplimiento Gestión de Activos Protección de Datos	Defensa	Los registros (logs accesos, auditorías, incidentes, riesgos) son evidencia crítica cumplimiento ISO27001 y requisitos legales (RGPD, DORA), requiriendo protección contra pérdida, alteración o divulgación no autorizada. Se aplica para garantizar integridad y disponibilidad registros organizacionales.	Los registros de las actividades del Sistema están protegidos por control de acceso físico y lógico. Se mantienen copias de seguridad para evitar pérdidas
A.5.34	Controles organizacionales	Privacidad y protección de datos de carácter personal (DCP)	Control La organización debe identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de datos de carácter personal (DCP) de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar Proteger	Protección de Datos Legal y Cumplimiento	Protección	La organización maneja datos personales de empleados y partes interesadas en procesos administrativos y operaciones, sujetos a RGPD/LOPD. Se aplica para identificar y cumplir requisitos legales de privacidad y protección DCP aplicables al SGI.	La organización identifica y gestiona los tratamientos de datos de carácter personal que realiza, teniendo en cuenta los requisitos legales, regulatorios, contractuales y las instrucciones aplicables. Se aplican medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como controles de acceso, conservación y eliminación conforme a los plazos establecidos. Asimismo, se gestionan los derechos de las personas interesadas, las solicitudes de información y, cuando corresponde, las violaciones de seguridad de los datos personales. El cumplimiento de los requisitos de privacidad y protección de datos se revisa periódicamente y se actualiza cuando se producen cambios normativos, organizativos o en los tratamientos realizados.
A.5.35	Controles organizacionales	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidos los procesos, la tecnología y las personas, debe revisarse de forma independiente a intervalos planificados o siempre que se produzcan cambios significativos.	Aplica	Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Identificar Proteger	Seguridad de la Información	Gobernanza y ecosistema Protección	Las auditorías son un proceso independiente que permite reconocer el cumplimiento de la organización con requisitos asociados a la seguridad de la infromación	Se dispone del procedimiento Auditoria interna, se planifican y registran las auditorias. En la actualidad, las auditorías internas del SGI se realizan por parte de una consultoría externa. Por otra parte las auditorías de certificación se realizan por una entidad acreditada.
A.5.36	Controles organizacionales	Cumplimiento de las políticas y normas de seguridad de la información	Control Debe comprobarse periódicamente el cumplimiento con la política de seguridad de la información, las políticas temáticas específicas, las reglas y las normas de la organización.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar Proteger	Legal y Cumplimiento Seguridad de la Información	Gobernanza y ecosistema Protección	La revisión del cumplimiento de las políticas y normas permite conocer la eficacia del SGI	El cumplimiento de las políticas, procedimientos y normas internas de seguridad de la información se verifica periódicamente mediante auditorías, revisiones y controles específicos. Los resultados se documentan y las desviaciones identificadas se gestionan mediante acciones correctivas y de mejora, cuyo seguimiento se realiza hasta su cierre.
A.5.37	Controles organizacionales	Documentación de procedimientos operacionales	Control Deben documentarse los procedimientos operacionales de los medios de tratamiento de la información y ponerse a disposición de todos los usuarios que los necesiten.	Aplica	Preventivo Correctivo	Confidencialidad Integridad Disponibilidad	Proteger Recuperar	Gestión de Activos Securidad Física Securidad y Red - Trabajo Seguridad Aplicaión seguridad Configuración Segura Identidad y Gestión Acceso Amenaza y Vulnerabilidad - Administracion Continuidad Gestión Información y Eventos Seguridad	Gobernanza y ecosistema Protección Defensa	Los procedimientos operacionales aseguran aplicación consistente de controles SGSI en todos los procesos organizacionales, evitando desviaciones que comprometan seguridad información. Se aplica para documentar y disponibilizar procedimientos necesarios a usuarios responsables.	Se dispone de procedimientos operativos documentados, actualizados y accesibles para los usuarios que los necesitan según su función. Estos procedimientos se prueban periódicamente para verificar su adecuación y aplicabilidad, registrándose los resultados y las acciones de mejora cuando corresponde.

Control Anexo A	Grupo	Nombre	Descripción	Aplicación/Excluído	Tipo de control	Información (propiedades seguridad)	Conceptos	Operacional Capacidades	Dominios de Seguridad	Justificación	Gestión
A.6.1	Personas	Comprobación	Control La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo antes de unirse a la organización y de forma continua, de acuerdo con las leyes, reglamentos y éticas aplicables, y debe ser proporcional a los requisitos empresariales, la clasificación de la información a la que se accederá y los riesgos percibidos.	Aplica	Identificativo	Confidencialidad Integridad Disponibilidad	Proteger	Recursos Humanos Seguridad	Gobernanza y ecosistema Protección	El personal accede a información privada de negocio y confidencial de empleados, requiriendo verificación de antecedentes proporcional a riesgos y clasificación de activos. Se aplica el control conforme a legislación laboral española y análisis de riesgos del SGI	Antes de la incorporación, se realizan comprobaciones de referencias laborales de los candidatos, de acuerdo con la legislación aplicable y de forma proporcional a las responsabilidades del puesto, el nivel de acceso previsto y la sensibilidad de la información tratada.
A.6.2	Personas	Términos y condiciones de contratación	Control Los acuerdos contractuales de empleo deben indicar las responsabilidades del personal y de la organización en materia de seguridad de la información.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Recursos Humanos Seguridad	Gobernanza y ecosistema Protección	Los contratos deben explicitar responsabilidades en seguridad de la información para garantizar compromiso del personal. Se aplica el control para incluir cláusulas específicas en acuerdos laborales según políticas del SGI.	Los empleados firman clausulas de confidencialidad al comienzo de la relación contractual. Al inicio de la relación laboral al empleado se le facilita las políticas del Sistema y la política de seguridad del empleado. Además, se hacen campañas de concienciación. Se incluyen epígrafes en la clausula de confidencialidad del empleado para evitar la fuga de informacion una vez el empleado abandona la empresa o por cese de contrato. A la finalización de la relacion contractual, el Responsable de Seguridad retira los accesos a dicho empleado.
A.6.3	Personas	Concienciación, educación y formación en seguridad de la información	Control El personal de la organización y las partes interesadas pertinentes deben recibir una adecuada concienciación, educación y formación sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización y de las políticas y los procedimientos específicos, según corresponda a su puesto de trabajo.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Recursos Humanos Seguridad	Gobernanza y ecosistema Protección	El personal requiere competencias actualizadas en seguridad para prevenir incidentes operativos. Se aplica el control para proporcionar formación adaptada a roles y políticas del SGSI, con actualización periódica.	Se dispone de una formación en materia de seguridad de la información que se ha desplegado a toda la organización, y que será ampliada periódicamente mediante píldoras formativas. Esta formación se incluye en la documentación suministrada a las nuevas incorporaciones.
A.6.4	Personas	Proceso disciplinario	Control Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados y partes interesadas pertinentes, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	Aplica	Correctivo	Confidencialidad Integridad Disponibilidad	Proteger Responder	Recursos Humanos Seguridad	Gobernanza y ecosistema Protección	Las violaciones de seguridad requieren aplicación consistente de sanciones para disuadir incumplimientos. Se aplica el control para formalizar proceso disciplinario comunicado al personal.	Existe un proceso disciplinario que se aplicaría en función de la infracción cometida.
A.6.5	Personas	Responsabilidad ante la finalización o cambio	Control Las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cese o cambio de empleo se deben definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Recursos Humanos Seguridad Gestión de Activos	Gobernanza y ecosistema Protección	Las obligaciones de seguridad persisten post-cese/cambio de rol para proteger información privada. Se aplica el control para definir y comunicar responsabilidades continuas.	Los permisos de acceso se eliminan en la finalización del empleo. En el caso de cambiar de puesto dentro de la empresa se otorga permisos de acceso a los nuevos sistemas si fuera necesario.
A.6.6	Personas	Acuerdos de confidencialidad o no divulgación	Control Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la información de la organización deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes.	Aplica	Preventivo	Confidencialidad	Proteger	Recursos Humanos Seguridad Protección de Datos Relación Proveedores	Gobernanza y ecosistema Protección	Información privada de negocio y empleados requiere protección contractual explícita. Se aplica el control para identificar, documentar y firmar acuerdos de confidencialidad con personal y partes externas pertinentes.	Todos los contratos con terceras partes y personal son revisados y contienen acuerdos de confidencialidad, de acuerdo con la RGPD. Con los clientes se firman acuerdos de confidencialidad contenidos en el propio contrato.
A.6.7	Personas	Teletrabajo	Control Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Protección de Datos Gestión de Activos Seguridad Física Sistema y red - Trabajo Seguridad	Gobernanza y ecosistema Protección	El teletrabajo expone información privada a riesgos en entornos no controlados. Se aplica el control para proteger datos accedidos/procesados desde ubicaciones remotas.	Existe una política específica sobre el teletrabajo comunicada y aprobada.
A.6.8	Personas	Notificación de los eventos de seguridad de la información	Control La organización debe proporcionar un mecanismo para que el personal notifique a tiempo eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.	Aplica	Detectivo	Confidencialidad Integridad Disponibilidad	Detectar	Gestión Información y Eventos Seguridad	Defensa	La detección temprana de incidentes depende de notificación fluida por parte del personal. Se aplica el control para proporcionar mecanismos accesibles de reporte de eventos observados/sospechosos.	Todo el personal debe notificar, tan pronto como sea posible, cualquier evento o debilidad de seguridad de la información observada o sospechada mediante los canales establecidos por la organización. Las notificaciones se gestionan y registran para su evaluación y seguimiento conforme al procedimiento de gestión de incidentes.
A.7.1	Infraestructura	Perímetro de seguridad física	Control Se deben definir y utilizar perímetros de seguridad para proteger áreas que contengan información y otros activos asociados.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física	Protección	Las áreas que contienen información privada de negocio y equipos críticos requieren protección contra accesos físicos no autorizados. Se aplica el control para definir perímetros de seguridad física en oficina y CPD, según el análisis de riesgos del SGI.	La organización dispone de perímetros de seguridad física definidos para proteger sus instalaciones y los activos asociados. El acceso a las áreas protegidas se controla y se limita al personal autorizado, de acuerdo con las necesidades de seguridad de la organización.
A.7.2	Infraestructura	Controles físicos de entrada	Control Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física Gestión Información y Eventos Seguridad	Protección	Los accesos físicos no controlados a áreas con información y equipos sensibles comprometen la confidencialidad. Se aplica el control para proteger CPD y zonas con activos críticos mediante controles de entrada adecuados.	Las áreas seguras disponen de controles físicos de entrada que restringen el acceso al personal autorizado. Las visitas y personas externas son supervisadas durante su permanencia en las instalaciones, aplicándose medidas de acompañamiento cuando corresponde. Los accesos se gestionan de acuerdo con las necesidades de seguridad de cada área y los riesgos asociados.
A.7.3	Infraestructura	Seguridad de oficinas, despachos y recursos	Control Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física Gestión de Activos	Protección	Las oficinas, despachos y recursos cuentan con protección física frente a terceros, mediante un control de acceso en la entrada	La oficina, despachos y áreas que contienen información o activos relevantes disponen de medidas de seguridad física adecuadas a los riesgos identificados. Estas medidas incluyen controles de acceso y restricciones para evitar el acceso no autorizado. La seguridad física se mantiene y revisa cuando se producen cambios en las instalaciones, los activos o las necesidades de protección.
A.7.4	Infraestructura	Monitorización de la seguridad física	Control Las instalaciones deben ser monitorizadas continuamente para detectar cualquier acceso físico no autorizado.	Aplica	Detectivo Proteger	Confidencialidad Integridad Disponibilidad	Proteger Detectar	Seguridad Física	Protección Defensa	La detección oportuna de accesos físicos no autorizados protege instalaciones y activos sensibles.	La seguridad física de las instalaciones se monitoriza mediante los controles establecidos para detectar accesos no autorizados. Los eventos identificados se comunican y gestionan a través de los canales definidos.

Control Anexo A	Grupo	Nombre	Descripción	Aplicación/Excluído	Tipo de control	Información (propiedades seguridad)	Conceptos	Operacional Capacidades	Dominios de Seguridad	Justificación	Gestión
A.7.5	Infraestructura	Protección contra las amenazas físicas y ambientales	Control Se debe diseñar e implementa una protección a las infraestructuras contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionadas o no.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física	Protección	Las amenazas físicas y ambientales pueden afectar disponibilidad de CPD y continuidad operativa según BIA. Se aplica el control para proteger infraestructura contra incendios, temperatura y otros riesgos.	Las instalaciones disponen de medidas de protección frente a amenazas físicas y ambientales, incluyendo sistemas de protección contra incendios y planes de evacuación. Asimismo, se cuenta con medidas de continuidad para facilitar la recuperación de las actividades en caso de una emergencia. Estas medidas se revisan y mantienen de acuerdo con las necesidades de la organización.
A.7.6	Infraestructura	El trabajo en áreas seguras	Control Se debe diseñar e implementar procedimientos para trabajar en las áreas seguras.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física	Protección	La regulación del acceso y de los trabajos en áreas seguras reduce el riesgo de accesos no autorizados, daños físicos y afectación a la información o a los activos asociados.	El acceso y los trabajos en áreas seguras requieren autorización previa y se realizan conforme a procedimientos establecidos. Se mantienen registros de acceso y, cuando procede, se requiere acompañamiento durante la intervención. Asimismo, se aplican normas de seguridad específicas y se evita la realización de trabajos en solitario cuando exista un riesgo asociado.
A.7.7	Infraestructura	Puesto de trabajo despejado y pantalla limpia	Control Deben definirse y hacerse cumplir reglas de puesto de trabajo despejado de papeles y de medios de almacenamiento removibles, así como reglas de pantalla limpia para los recursos de tratamiento de la información.	Aplica	Preventivo	Confidencialidad	Proteger	Seguridad Física	Protección	Las condiciones de los puestos de trabajo deben ser tal que no permitan que las vulnerabilidades del sistema sean aprovechadas	Se establecen y comunican normas de puesto de trabajo despejado y pantalla limpia, aplicables a todo el personal. Estas normas incluyen la custodia adecuada de documentos y medios de almacenamiento, el bloqueo de la pantalla cuando el puesto queda desatendido y la retirada de la información cuando ya no es necesaria. Su cumplimiento se promueve mediante la comunicación y concienciación del personal.
A.7.8	Infraestructura	Emplazamiento y protección de equipos	Control Los equipos deben situarse de forma protegida y segura.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física Gestión de Activos	Protección	Los equipos críticos requieren ubicación protegida contra amenazas físicas y ambientales. Se aplica el control para emplazamiento seguro de servidores y equipos sensibles.	Los equipos y activos tecnológicos se ubican en emplazamientos protegidos frente a accesos no autorizados, robo, daños accidentales y amenazas físicas o ambientales. Se aplican medidas adecuadas según la criticidad del equipo, como control de las condiciones ambientales, protección frente a sobretensiones y fijación o ubicación segura de los equipos de oficina. Estas medidas se revisan teniendo en cuenta los riesgos identificados y los requisitos de continuidad.
A.7.9	Infraestructura	Seguridad de los equipos fuera de las instalaciones	Control Los activos fuera de las instalaciones deben estar protegidos.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física Gestión de Activos	Protección	El teletrabajo con equipos portátiles expone datos privados a riesgos físicos/remotos. Se aplica el control para proteger activos fuera de instalaciones según política de dispositivos móviles.	Todos los equipos están protegidos por contraseña. Existe una política específica para el uso de equipos fuera de las instalaciones.
A.7.10	Infraestructura	Soportes de almacenamiento	Control Los soportes de almacenamiento deben gestionarse durante todo su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física Gestión de Activos	Protección	Los soportes con datos internos requieren gestión segura durante su ciclo de vida completo. Se aplica el control según clasificación de activos y políticas de eliminación	Se mantiene inventario de soportes de almacenamiento con clasificación de datos. Al final de su ciclo de vida útil, se aplica eliminación segura mediante sobrescritura (software especializado) o destrucción física certificada, con registro documentado del proceso y responsables.
A.7.11	Infraestructura	Instalaciones de suministro	Control Las instalaciones de procesamiento de información deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	Aplica	Preventivo Detectivo	Integridad Disponibilidad	Proteger Detectar	Seguridad Física	Protección	Los fallos o interrupciones en las instalaciones de suministro pueden afectar a la disponibilidad, integridad y funcionamiento de los activos críticos. Por ello, se aplican medidas de protección acordes con los requisitos de continuidad y los riesgos identificados.	Los activos críticos disponen de medidas de protección frente a fallos o interrupciones de las instalaciones de suministro, incluyendo sistemas de alimentación ininterrumpida cuando resulta necesario. Estas medidas permiten mantener la operación durante el tiempo requerido o realizar un cierre ordenado de los sistemas, de acuerdo con los objetivos de continuidad establecidos.
A.7.12	Infraestructura	Seguridad del cableado	Control El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	Aplica	Preventivo	Confidencialidad Disponibilidad	Proteger	Seguridad Física	Protección	El cableado eléctrico y de telecomunicaciones puede verse afectado por daños físicos, interferencias o accesos no autorizados, comprometiendo la disponibilidad y confidencialidad de la información. Por ello, se aplican medidas de protección adecuadas a su función y ubicación.	El cableado eléctrico y de telecomunicaciones se instala y mantiene de forma protegida, utilizando canalizaciones y medidas físicas adecuadas. Cuando corresponde, se separan los distintos tipos de cableado y se limita su exposición a accesos no autorizados, reduciendo el riesgo de daños, interferencias o interceptaciones.
A.7.13	Infraestructura	Mantenimiento de los equipos	Control Los equipos deben recibir un mantenimiento correcto que asegure la disponibilidad, integridad y confidencialidad de la información.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física Gestión de Activos	Protección Resiliencia	Se establecen prácticas para el mantenimiento de los equipos como laptops, con el fin de garantizar su desempeño en el tiempo	Los equipos reciben una revisión al menos anual y mantenimiento adicional cuando resulta necesario. Las intervenciones son realizadas por personal autorizado y se gestionan de forma que se protejan la información y los activos tratados. Durante las revisiones se comprueba su estado, funcionamiento y protección frente a código malicioso.
A.7.14	Infraestructura	Eliminación o reutilización segura de equipos	Control Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia, han sido eliminados o sobrescritos de manera segura, antes de deshacerse de ellos o reutilizarlos.	Aplica	Preventivo	Confidencialidad	Proteger	Seguridad Física Gestión de Activos	Protección	Equipos retirados pueden contener datos residuales privados/confidenciales. Se aplica el control para eliminar datos seguros antes de disposición o reutilización.	Existen procedimientos específicos para la eliminación segura de equipos
A.8.1	Tecnología	Dispositivos finales de usuario	Control La información almacenada, procesada o accesible a través de dispositivos finales de usuario debe protegerse.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gestión de Activos Protección de Datos	Protección	Los dispositivos finales de usuario pueden almacenar/procesar datos privados y ser expuestos a riesgos físicos/remotos. Se aplica el control para proteger información en endpoints según políticas de uso y análisis de riesgos del SGI.	Se cuenta con políticas específicas sobre el uso adecuado de los dispositivos finales de usuario
A.8.2	Tecnología	Gestión de privilegios de acceso	Control La asignación y el uso de derechos de acceso con privilegios deben restringirse y controlarse.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gestión Información y Eventos Seguridad	Protección	Los privilegios de acceso elevados no controlados pueden permitir modificaciones no autorizadas o daños significativos en sistemas y datos privados. Se aplica el control para restringir y controlar asignación/uso de derechos privilegiados, según políticas de acceso y análisis de riesgos del SGI.	Se restringen privilegios elevados (administrador, root, sudo) al personal esencial mediante aprobaciones formales, principio de mínimo privilegio y autenticación multifactor cuando aplica. Se registran y auditan todas las operaciones privilegiadas, con revisiones periódicas de asignaciones y desconexión automática de sesiones inactivas.
A.8.3	Tecnología	Restricción del acceso a la información	Control Se debe restringir el acceso a la información y otros activos relacionados, de acuerdo con las políticas específicas de control de acceso definidas.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gestión Información y Eventos Seguridad	Protección	El acceso no restringido puede comprometer confidencialidad, integridad y disponibilidad de datos privados de negocio y empleados. Se aplica el control para restringir acceso según políticas específicas de control de acceso y análisis de riesgos del SGI.	Se implementa principio de mínimo privilegio en todos los sistemas, aplicaciones y datos, con accesos basados en roles y necesidad de conocer. Las políticas de control de acceso definen reglas claras de otorgamiento, revisión periódica y revocación de permisos, alineadas con autenticación segura, gestión de código fuente y segregación de entornos.

Control Anexo A	Grupo	Nombre	Descripción	Aplicación/Excluído	Tipo de control	Información (propiedades seguridad)	Conceptos	Operacional Capacidades	Dominios de Seguridad	Justificación	Gestión
A.8.4	Tecnología	Acceso al código fuente	Control Se debe gestionar adecuadamente el acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y Gestión Acceso Apicación Seguridad Configuración Seguridad	Protección	El acceso inadecuado al código fuente, herramientas de desarrollo y bibliotecas puede comprometer integridad y confidencialidad de propiedad intelectual. Se aplica el control para gestionar lectura/escritura adecuadamente, según el análisis de riesgos del SGI.	Se gestiona acceso al código fuente y herramientas mediante repositorios centralizados con controles basados en roles (lectura/escritura/admin), principio de mínimo privilegio y autenticación segura. Solo personal autorizado del equipo de desarrollo accede, con registros de cambios auditables, revisiones periódicas de permisos y alineación con gestión de cambios y desarrollo seguro.
A.8.5	Tecnología	Autenticación segura	Control Las tecnologías y procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica sobre control de acceso.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y Gestión Acceso	Protección	Autenticaciones débiles pueden permitir accesos no autorizados a sistemas y datos privados. Se aplica el control para implementar tecnologías y procedimientos de autenticación segura alineados con la política de control de acceso, según el análisis de riesgos del SGI	Se dispone de los mecanismos propios del Sistema Operativo. Se exige identificación y autenticación al iniciar sesión en los equipos informáticos. Existe una política de gestión de contraseñas, donde se recoge la periodicidad de las mismas y los requisitos de complejidad además de doble factor.
A.8.6	Tecnología	Gestión de capacidades	Control Se debe supervisar y ajustar la utilización de los recursos en consonancia con los requisitos de capacidad actuales y esperados.	Aplica	Preventivo Detectivo	Integridad Disponibilidad	Identificar Proteger Detectar	Continuidad	Gobernanza y ecosistema Protección	La utilización inadecuada de recursos puede afectar disponibilidad y rendimiento de sistemas críticos identificados en el BIA. Se aplica el control para supervisar y ajustar capacidades según requisitos actuales y previstos, conforme al análisis de riesgos del SGI.	Se monitoriza periódicamente la utilización de recursos (CPU, memoria, almacenamiento, ancho de banda) en sistemas clave, identificando tendencias y planificando capacidad futura. Los ajustes se realizan mediante gestión de cambios y se documentan para garantizar alineación con requisitos operativos y de continuidad.
A.8.7	Tecnología	Controles contra el código malicioso	Control Se debe implementar una protección contra el código malicioso, respaldada por una concienciación adecuada al usuario.	Aplica	Preventivo Detectivo Correctivo	Confidencialidad Integridad Disponibilidad	Proteger Detectar	Sistema y Red - Segurdad Protección de Datos	Protección Defensa	El código malicioso (virus, malware, ransomware) puede comprometer sistemas y datos privados de negocio/empleados. Se aplica el control para implementar protección técnica y concienciación del usuario, según el análisis de riesgos del SGI	Se implementan soluciones antivirus/anti-malware en endpoints y servidores, con actualizaciones automáticas de firmas y escaneos periódicos. Se complementa con filtrado web, políticas de uso de dispositivos y formación regular a usuarios sobre identificación de amenazas (phishing, adjuntos sospechosos). Los incidentes se gestionan mediante procedimientos formales.
A.8.8	Tecnología	Gestión de vulnerabilidades técnicas	Control: Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar Proteger	Amenaza y Vulnerabilidad - Administracion	Gobernanza y ecosistema Protección Defensa	Las vulnerabilidades técnicas no gestionadas pueden comprometer sistemas, redes y aplicaciones que procesan datos privados de negocio y empleados. Se aplica el control para obtener información, evaluar exposición y mitigar vulnerabilidades según el análisis de riesgos del SGI.	La organización obtiene información sobre vulnerabilidades técnicas mediante fuentes especializadas y realiza análisis periódicos de los sistemas y aplicaciones utilizados. Asimismo, cuando resulta aplicable, se realizan análisis estáticos del código fuente, análisis dinámicos de las aplicaciones y pruebas de penetración. Las vulnerabilidades identificadas se evalúan según su impacto y exposición, y se gestionan mediante correcciones, actualizaciones, parches o medidas compensatorias documentadas, integrándose en la gestión de cambios.e cambios.
A.8.9	Tecnología	Gestión de la configuración	Control Se debe establecer, documentar, implementar, monitorizar y revisar las configuraciones de hardware, software, servicios y redes, incluyendo sus configuraciones de seguridad.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Configuración Seguridad	Protección	Configuraciones inadecuadas o desactualizadas pueden exponer vulnerabilidades en hardware, software, servicios y redes. Se aplica el control para establecer, documentar e implementar gestión formal de configuraciones, según el análisis de riesgos del SGI.	Se utilizan configuraciones baselines seguras para hardware, software, servicios y redes, incluyendo parámetros de seguridad críticos. Se monitorizan desviaciones mediante revisiones periódicas y escaneos automatizados cuando aplicable, con corrección vía gestión de cambios. Los cambios de configuración requieren aprobación.
A.8.10	Tecnología	Eliminación de la información	Control La información almacenada en los sistemas de información, en los dispositivos y cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria.	Aplica	Preventivo	Confidencialidad	Proteger	Protección de Datos Legal y Cumplimiento		La retención innecesaria de información privada de negocio y confidencial de empleados genera riesgos de exposición. Se aplica el control para eliminar información cuando ya no es necesaria, según el análisis de riesgos del SGI y políticas de retención.	Se definen políticas de retención por tipo de información con procedimientos documentados de eliminación segura en sistemas, dispositivos y medios. La eliminación se ejecuta por personal autorizado, alineada con copias de seguridad.
A.8.11	Tecnología	Enmascaramiento de datos	Control El enmascaramiento de datos debe utilizarse de acuerdo con la política específica del tema de la organización sobre el control de acceso, con otras políticas temáticas relacionadas, así como con los requisitos de negocio, teniendo en cuenta los requisitos legales aplicables.	Excluído						El enmascaramiento de datos es una técnica utilizada para proteger datos confidenciales, especialmente información de identificación personal, mediante la alteración de los datos originales para que no puedan ser vinculados a las personas o entidades a las que pertenecen. Su objetivo es salvaguardar la información sensible más allá de los controles habituales, como el control de acceso, y se emplea habitualmente en entornos de desarrollo, pruebas o cuando se comparten datos con terceros. Las técnicas más comunes incluyen la seudonimización, la anonimización, la sustitución y el cifrado, entre otras, buscando siempre que los datos enmascarados mantengan el formato pero no permitan la identificación de los interesados. El control A.8.11 se considera no aplicable dado que, tras el análisis de riesgos, no se identifican datos sensibles en los entornos de desarrollo, prueba o soporte. Los únicos datos potencialmente sensibles, como nombres de usuario, no requieren enmascaramiento según el contexto y el marco legal vigente. La información sensible de recursos humanos está protegida mediante controles de acceso específicos. Esta decisión será revisada ante cualquier cambio relevante en los procesos o los datos tratados.	No aplica.
A.8.12	Tecnología	Prevención de fugas de datos	Control Se deben aplicar medidas de prevención de fugas de datos a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.	Aplica	Preventivo Detectivo	Confidencialidad	Proteger Detectar	Protección de Datos	Protección Defensa	La organización procesa datos privados de negocio y confidenciales de empleados, con riesgo de fugas no autorizadas. Se aplica el control para implementar medidas de prevención de fugas en sistemas, redes y dispositivos, según el análisis de riesgos del SGI	Se aplican políticas de uso aceptable de dispositivos que restringen almacenamiento/portabilidad de datos sensibles, junto con filtrado web que bloquea sitios de compartición de archivos no autorizados.
A.8.13	Tecnología	Copias de seguridad de la información	Control Las copias de seguridad de la información, del software y de los sistemas deben mantenerse y probarse periódicamente de acuerdo con la política de copias de seguridad específica acordada.	Aplica	Correctivo	Integridad Disponibilidad	Recuperar	Continuidad	Protección	La pérdida de información, software o sistemas críticos puede interrumpir operaciones y comprometer continuidad. Se aplica el control para mantener copias de seguridad probadas periódicamente, según el análisis de riesgos del SGI y requisitos del BIA.	Se realizan copias de seguridad periódicas de la información, el software y las configuraciones críticas. Estas copias se almacenan en el proveedor de servicios y en localizaciones alternativas, aplicando medidas de protección adecuadas. Periódicamente se verifica su integridad y capacidad de restauración, manteniendo los registros correspondientes.
A.8.14	Tecnología	Redundancia recursos de tratamiento de la información	Control Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	Aplica	Preventivo	Disponibilidad	Proteger	Continuidad Gestión de Activos	Protección Resiliencia	Los recursos críticos identificados en el análisis BIA requieren disponibilidad garantizada para cumplir objetivos operativos. Se aplica el control para implementar redundancia suficiente en recursos de tratamiento de información según los requisitos de disponibilidad determinados por el BIA.	Se identifican recursos críticos en el análisis BIA (Business Impact Analysis) con sus requisitos de disponibilidad (RTO/RPO). Para estos activos se implementan medidas de redundancia proporcionales (copia de seguridad, clustering, balanceadores cuando justificado por criticidad), documentadas en planes de continuidad. Los niveles de redundancia se verifican periódicamente mediante pruebas y auditorías internas, alineados con ISO 22301.

Control Anexo A	Grupo	Nombre	Descripción	Aplicación/Excluído	Tipo de control	Información (propiedades seguridad)	Conceptos	Operacional Capacidades	Dominios de Seguridad	Justificación	Gestión
A.8.15	Tecnología	Registros de eventos	Control Se deben generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes.	Aplica	Detectivo	Confidencialidad Integridad Disponibilidad	Detectar	Gestión Información y Eventos Seguridad	Protección Resiliencia	La ausencia de registros adecuados impide detectar, investigar y responder a incidentes de seguridad. Se aplica el control para generar, proteger y analizar logs de actividades relevantes, según el análisis de riesgos del SGI.	Se generan registros de eventos clave (accesos privilegiados, cambios, errores, operaciones críticas) en sistemas y aplicaciones, protegidos contra manipulación y almacenados centralizadamente con retención definida. Solo personal autorizado accede a logs (mínimo privilegio), que se revisan periódicamente y se usan para investigaciones de incidentes y cumplimiento.
A.8.16	Tecnología	Seguimiento de actividades	Control Las redes, los sistemas y las aplicaciones deben monitorizarse en busca de comportamientos anómalos y se deben tomar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.	Aplica	Detectivo Correctivo	Confidencialidad Integridad Disponibilidad	Detectar Proteger	Gestión Información y Eventos Seguridad	Defensa	Comportamientos anómalos no detectados pueden indicar incidentes de seguridad no identificados. Se aplica el control para monitorizar redes, sistemas y aplicaciones, evaluando posibles incidentes según el análisis de riesgos del SGI.	Se monitorizan periódicamente redes, sistemas y aplicaciones clave buscando anomalías (uso excesivo de recursos, accesos inusuales, patrones sospechosos), utilizando herramientas estándar y alertas configuradas. Cualquier indicio se evalúa formalmente mediante procedimientos de incidentes, con escalado según criticidad y documentación de medidas tomadas.
A.8.17	Tecnología	Sincronización del reloj	Control Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con fuentes de tiempo aprobadas.	Aplica	Detectivo	Integridad	Proteger Detectar	Gestión Información y Eventos Seguridad	Protección Defensa	Los relojes desincronizados dificultan la correlación precisa de eventos en logs, investigaciones de incidentes y trazabilidad operativa. Se aplica el control para sincronizar relojes de sistemas con fuentes de tiempo fiables, según el análisis de riesgos del SGI.	Estan sincronizados automaticamente
A.8.18	Tecnología	Uso de los programas de utilidad con privilegios	Control Se debe restringir y controlar rigurosamente el uso de programas de utilidad que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Aplicación Seguridad Sistema y Red - Trabajo Seguridad Configuración Seguridad	Protección	Los programas de utilidad con privilegios elevados pueden eludir controles de seguridad si se usan sin restricciones, afectando integridad y confidencialidad de sistemas y datos internos. Se aplica el control para restringir y controlar su uso riguroso, según el análisis de riesgos del SGI.	Se restringe el uso de utilidades privilegiadas (como sudo, scripts administrativos) al personal autorizado mediante principio de mínimo privilegio, con aprobaciones documentadas y registros de auditoría habilitados. Su empleo sigue procedimientos formales alineados con gestión de cambios, con revisiones periódicas de accesos y monitoreo de uso anómalo.
A.8.19	Tecnología	Instalación del software en sistemas en producción	Control Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas en producción.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Configuración Seguridad Aplicación Seguridad	Protección	Las instalaciones de software en sistemas en producción pueden introducir vulnerabilidades o interrupciones del servicio si no se gestionan adecuadamente. Se aplica el control para asegurar que los despliegues en producción se realizan de forma controlada y segura, conforme al análisis de riesgos del SGI.	Están restringidas las instalaciones de software en los equipos. Cualquier cambio al equipo debe ser permitido por la autoridad correspondiente, y sólo los administradores tienen los privilegios necesarios para realizar la instalación de software.
A.8.20	Tecnología	Seguridad de redes	Control Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.	Aplica	Preventivo Detectivo	Confidencialidad Integridad Disponibilidad	Proteger Detectar	Sistema y Red - Segurdad	Protección	Las redes y dispositivos sin protección adecuada pueden exponer información interna y sistemas a accesos no autorizados o ataques. Se aplica el control para proteger, gestionar y controlar redes según el análisis de riesgos del SGI	Se protegen redes y dispositivos mediante firewalls perimetrales, actualizaciones regulares de firmware/patches, controles de acceso restringidos (mínimo privilegio) y segregación lógica. Se gestionan configuraciones mediante procedimientos documentados y se monitorizan periódicamente anomalías de tráfico. Cualquier modificación sigue gestión de cambios.
A.8.21	Tecnología	Seguridad de los servicios de red	Control Se deben identificar, implementar y monitorizar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de todos los servicios de red.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Sistema y Red - Segurdad	Protección	Los servicios de red sin controles adecuados pueden exponer vulnerabilidades que afecten disponibilidad, integridad y confidencialidad de sistemas y datos internos. Se aplica el control para identificar, implementar y monitorizar medidas de seguridad en todos los servicios de red, según el análisis de riesgos del SGI	Se identifican los servicios de red críticos con requisitos de seguridad y niveles de servicio documentados. Se aplican controles estándar (firewalls, cifrado TLS, autenticación) y se monitorizan periódicamente para verificar funcionamiento y cumplimiento
A.8.22	Tecnología	Segregación en redes	Control Los grupos de servicios de información, de usuarios y de sistemas de información deben ser segregados en las redes de la organización.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Sistema y Red - Segurdad	Protección	La falta de segregación puede permitir que una brecha en un segmento afecte toda la red, comprometiendo confidencialidad, integridad y disponibilidad de sistemas y datos internos. Se aplica el control para segregar grupos de servicios/usuarios/sistemas, según el análisis de riesgos del SGI.	Se implementa segregación lógica/física de redes que separa entornos de desarrollo, pruebas, producción y funciones administrativas, usando VLANs, firewalls o zonas de confianza diferenciadas. Los accesos entre segmentos requieren autorización explícita por principio de mínimo privilegio, con monitoreo de tráfico y revisiones periódicas de reglas. Se alinea con controles de acceso.
A.8.23	Tecnología	Filtrado de webs	Control El acceso a sitios web externos debe gestionarse para reducir la exposición a contenido malicioso.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Sistema y Red - Segurdad	Protección	El acceso no controlado a sitios web externos puede exponer a malware, phishing o contenido malicioso que afecte sistemas internos. Se aplica el control para gestionar y filtrar accesos web, minimizando riesgos según el análisis del SGI.	Se implementan mecanismos de filtrado web que bloquean sitios conocidos maliciosos, categorías de alto riesgo (malware, phishing) y limitan navegación no esencial durante horario laboral. Los controles se aplican uniformemente a todos los dispositivos corporativos, con excepciones justificadas y aprobadas. Se complementa con concienciación en seguridad.
A.8.24	Tecnología	Uso de la criptografía	Control Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida para la gestión de claves criptográficas.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Configuración Seguridad	Protección	El manejo inadecuado de criptografía puede comprometer la confidencialidad e integridad de datos internos de la compañía en tránsito/reposo. Se aplica el control para definir reglas de uso eficaz y gestión de claves, según el análisis de riesgos del SGI.	Se definen políticas para el uso de criptografía estándar en comunicaciones (TLS), almacenamiento y protección de datos, con selección de algoritmos robustos y actualizaciones periódicas. Se implementan procedimientos documentados para generación, distribución, almacenamiento y rotación de claves criptográficas, con accesos restringidos por principio de mínimo privilegio. El cumplimiento se verifica en revisiones de seguridad y auditorías internas.
A.8.25	Tecnología	Seguridad en el ciclo de vida del desarrollo	Control Se deben establecer y aplicar reglas para el desarrollo seguro de aplicaciones y sistemas.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Aplicación Seguridad Sistema y Red - Trabajo Seguridad	Protección	El desarrollo de aplicaciones y sistemas sin reglas de seguridad integradas puede generar vulnerabilidades persistentes. Se aplica el control para establecer y aplicar reglas formales en todo el ciclo de vida, según el análisis de riesgos del SGI.	Se implementa una política de desarrollo seguro que define reglas obligatorias para todas las fases del ciclo de vida (diseño, codificación, pruebas, despliegue, mantenimiento), incorporando OWASP Top 10 y principios de ingeniería segura. Los desarrolladores con competencias verificadas aplican estas reglas mediante revisiones de código, pruebas automatizadas/manuales de seguridad, gestión de cambios y documentación de trazabilidad. Se realiza verificación continua de cumplimiento.
A.8.26	Tecnología	Requisitos de seguridad de las aplicaciones	Control Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Aplicación Seguridad Sistema y Red - Trabajo Seguridad	Protección Defensa	Las aplicaciones sin requisitos de seguridad explícitos pueden presentar vulnerabilidades inherentes. Se aplica el control para definir y documentar requisitos de seguridad específicos por aplicación, según el análisis de riesgos del SGI.	Dentro de las buenas prácticas de desarrollo seguro se contempla la adecuada recopilación de requisitos de seguridad para los desarrollos
A.8.27	Tecnología	Arquitectura segura de sistemas y principios de ingeniería	Control Los principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicar a todas las actividades de desarrollo de sistemas de información.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Aplicación Seguridad Sistema y Red - Trabajo Seguridad	Protección	Los diseños de sistemas inadecuados pueden introducir vulnerabilidades estructurales difíciles de mitigar posteriormente. Se aplica el control para incorporar principios de diseño seguro desde las primeras fases, según el análisis de riesgos del SGI y alineado con prácticas de desarrollo seguro.	Se aplican principios de ingeniería segura en el diseño de sistemas y software, documentados en especificaciones iniciales. La política de desarrollo seguro guía la identificación temprana de requisitos de seguridad (OWASP Top 10), con revisiones de diseño por equipo competente antes de avanzar fases. Se integra con pruebas de seguridad y gestión de cambios.

Control Anexo A	Grupo	Nombre	Descripción	Aplicación/Excluído	Tipo de control	Información (propiedades seguridad)	Conceptos	Operacional Capacidades	Dominios de Seguridad	Justificación	Gestión
A.8.28	Tecnología	Codificación segura	Control Principios de codificación segura deben aplicarse al desarrollo de software.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Aplicación Seguridad Sistema y Red - Trabajo Seguridad	Protección	El desarrollo de software puede introducir vulnerabilidades si no sigue reglas estandarizadas de seguridad. Se aplica el control para establecer y cumplir reglas de desarrollo seguro, mitigando riesgos identificados en el análisis del SGS, considerando actividades de desarrollo interno.	Se cuenta con una política formal de desarrollo seguro que incluye directrices basadas en OWASP Top 10, aplicada en todo el ciclo de vida del software. Los desarrolladores, con competencias verificadas y formación continua en prácticas seguras, siguen estas reglas mediante revisiones de código, pruebas de seguridad y alineación con gestión de cambios.
A.8.29	Tecnología	Pruebas de seguridad en desarrollo y aceptación	Control Deben definirse e implementarse procesos de pruebas de seguridad en el ciclo de vida del desarrollo.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Aplicación Seguridad Sistema y Red - Trabajo Seguridad	Protección	Las vulnerabilidades no detectadas en desarrollo pueden propagarse a producción, afectando confidencialidad, integridad y disponibilidad. Se aplica el control para definir e integrar pruebas de seguridad en el ciclo de desarrollo y aceptación, según el análisis de riesgos del SGI.	Se definen procesos de pruebas de seguridad (análisis estático/dinámico, revisiones de código) integrados en las fases de desarrollo y aceptación, realizados en entornos separados de producción. Las pruebas verifican el cumplimiento de requisitos de seguridad antes de los despliegues, con documentación de resultados, remediación de hallazgos y aprobaciones formales. Se alinea con gestión de cambios.
A.8.30	Tecnología	Externalización del desarrollo	Control La organización debe controlado, monitorizar y revisar las actividades relativas al desarrollo externalizado de sistemas.	Excluído						El control A.8.30 se considera no aplicable en la organización, dado que todas las actividades de desarrollo de software se realizan internamente, sin subcontratación ni participación de terceros. Por tanto, no existen riesgos asociados a la externalización que requieran la implementación de controles específicos para proveedores externos. Esta decisión será revisada en caso de que se modifique la estrategia de desarrollo y se contemple la externalización.	No aplica.
A.8.31	Tecnología	Separación de los entornos de desarrollo, prueba y producción	Control Deben separarse y protegerse los entornos de desarrollo, prueba y producción.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Aplicación Seguridad Sistema y Red - Trabajo Seguridad	Protección	Las actividades de desarrollo y pruebas pueden comprometer la integridad, disponibilidad o confidencialidad de los sistemas en producción. Se aplica el control para mantener entornos separados, según el análisis de riesgos del SGI y alineado con la política de protección de información en pruebas.	Se mantienen entornos lógicamente o físicamente separados para desarrollo, pruebas y producción, con controles de acceso diferenciados por principio de mínimo privilegio y revisiones periódicas.
A.8.32	Tecnología	Gestión de cambios	Control Los cambios en las instalaciones de tratamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Aplicación Seguridad Sistema y Red - Trabajo Seguridad	Protección	Los cambios en sistemas y entornos de información pueden introducir vulnerabilidades o interrupciones no planificadas. Se aplica el control para gestionar formalmente estos cambios, minimizando riesgos a la confidencialidad, integridad y disponibilidad según el análisis de riesgos del SGI.	Se sigue un procedimiento documentado de gestión de cambios que cubre planificación, evaluación de impacto y riesgos, aprobación por responsables, pruebas en entornos no productivos, implementación controlada y verificación post-cambio con registros auditables. Se asegura separación de entornos desarrollo/pruebas/producción, principio de mínimo privilegio y opciones de rollback. Todos los cambios significativos mantienen trazabilidad completa.
A.8.33	Tecnología	Datos de prueba	Control Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Protección de Datos	Protección	Los desarrollos manejan datos internos de la compañía en entornos de prueba, con riesgo de exposición no autorizada o uso inadecuado. Se aplica el control para seleccionar cuidadosamente, proteger y controlar los datos de prueba, según el análisis de riesgos del SGI.	La información de prueba se selecciona y gestiona según su nivel de sensibilidad y criticidad, conforme a la clasificación de activos. Dado que no se tratan datos personales, confidenciales o especialmente protegidos, se permite el uso de datos reales en entornos de prueba con medidas de seguridad generales, acceso restringido al personal autorizado (principio de mínimo privilegio, revisado periódicamente) y separación estricta de entornos desarrollo/pruebas/producción. Al finalizar las pruebas, los datos se eliminan de forma segura según procedimientos internos.
A.8.34	Tecnología	Protección de los sistemas de información durante las pruebas de auditoría	Control Las pruebas de auditoría y otras actividades de aseguramiento en la evaluación de los sistemas en producción deben ser cuidadosamente planificadas y acordadas entre el evaluador y los gestores adecuados.	Aplica	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Sistema y Red - Segurdad Protección de Datos	Gobernanza y ecosistema Protección	Se identifica riesgo de interrupciones o exposiciones durante auditorías en sistemas de producción. Control aplicable para garantizar continuidad operativa y confidencialidad de datos de clientes.	Las pruebas de auditoría y las actividades de aseguramiento se planifican, autorizan y coordinan previamente con los responsables correspondientes, definiendo su alcance y las medidas necesarias para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información.