Tipos de Control	Categoría	Control	Descripción	Aplicabilidad	Justificación
5. Controles Organizacionales	5.1	Políticas de seguridad de la información	Establecer políticas que definan cómo proteger la información.	APLICA	Es fundamental para definir un marco de seguridad alineado con los objetivos organizacionales.
	5.2	Roles y responsabilidades de seguridad de la información	Definir roles claros para gestionar la seguridad.	APLICA	Permite la asignación de responsabilidades específicas para una mejor gestión de riesgos.
	5.3	Separación de funciones	Evitar conflictos de interés mediante roles separados.	APLICA	Reduce el riesgo de fraude o acceso no autorizado al establecer funciones diferenciadas.
	5.4	Responsabilidades de gestión	Asegurar que los gestores asuman la seguridad.	APLICA	Los líderes deben garantizar el cumplimiento de las políticas de seguridad.
	5.5	Contacto con las autoridades	Formalizar acuerdos con autoridades relevantes.	APLICA	Facilita la comunicación y cumplimiento con organismos reguladores.
	5.6	Contacto con grupos de interés especial	Formalizar acuerdos de seguridad con terceros.	APLICA	Ayuda a compartir información y mejores prácticas en ciberseguridad.
	5.7	Inteligencia de amenazas	Monitorear y responder a amenazas emergentes.	APLICA	Permite anticiparse a riesgos y mejorar la postura de seguridad.
	5.8	Seguridad de la información en la gestión de proyectos	Incorporar seguridad en la gestión de proyectos.	APLICA	Garantiza que los proyectos contemplen medidas de seguridad desde su inicio.
	5.9	Inventario de información y otros activos asociados	Identificar y proteger activos clave.	APLICA	Un inventario actualizado permite una mejor gestión y protección de activos críticos.
	5.10	Uso aceptable de la información y otros activos asociados	Definir reglas de uso permitido de activos.	APLICA	Evita mal uso de recursos y establece pautas claras para los usuarios.
	5.11	Devolución de activos	Garantizar la recuperación de activos al finalizar relaciones laborales.	APLICA	Reduce el riesgo de fuga de información o uso indebido de recursos tras la desvinculación de empleados.
	5.12	Clasificación de la información	Clasificar la información según su sensibilidad.	APLICA	Permite establecer controles adecuados según el nivel de criticidad de la información.
	5.13	Etiquetado de información	Etiquetar datos para indicar su clasificación.	APLICA	Facilita el manejo seguro de la información conforme a su clasificación.
	5.14	Transferencia de información	Proteger la información durante su transferencia.	APLICA	Asegura la confidencialidad e integridad de la información transmitida.
	5.15	Control de acceso	Restringir el acceso a la información según roles.	APLICA	Minimiza riesgos al garantizar que solo usuarios autorizados accedan a la información.
	5.16	Gestión de identidad	Asegurar la gestión adecuada de identidades.	APLICA	Mejora la seguridad al controlar el acceso de los usuarios a los sistemas.
	5.17	Información de autenticación	Proteger las credenciales de autenticación.	APLICA	Reduce el riesgo de acceso no autorizado mediante credenciales seguras.
	5.18	Derechos de acceso	Asegurar que los accesos estén basados en necesidad.	APLICA	Limita la exposición de información solo a quienes lo requieran para sus funciones.
	5.19	Seguridad de la información en las relaciones con los proveedores	Gestionar riesgos en la colaboración con proveedores.	APLICA	Evita posibles brechas de seguridad derivadas de terceros.
	5.20	Abordar la seguridad de la información en los acuerdos con los proveedores	Proteger la información a lo largo de la cadena de suministro.	APLICA	Asegura que los proveedores cumplan con estándares de seguridad adecuados.
	5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Asegurar cambios seguros en los servicios de TI.	APLICA	Reduce riesgos asociados a terceros en la infraestructura tecnológica.
	5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	Supervisar y auditar cambios en los servicios contratados.	APLICA	Permite evaluar el impacto de los cambios en la seguridad de la información.
	5.23	Seguridad de la información para el uso de servicios en la nube	Proteger información almacenada o procesada en la nube.	APLICA	Reduce el riesgo de exposición o pérdida de datos en entornos cloud.
	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Prepararse para gestionar incidentes de seguridad.	APLICA	Garantiza una respuesta rápida y efectiva ante incidentes de seguridad.
	5.25	Evaluación y decisión sobre eventos de seguridad de la información	Evaluar eventos para decidir acciones apropiadas.	APLICA	Facilita la toma de decisiones basada en riesgos y amenazas identificadas.
	5.26	Respuesta a incidentes de seguridad de la información	Responder adecuadamente a incidentes de seguridad.	APLICA	Minimiza el impacto de incidentes mediante un plan de respuesta estructurado.
	5.27	Aprender de los incidentes de seguridad de la información	Usar lecciones aprendidas para prevenir futuros incidentes.	APLICA	Permite mejorar continuamente la postura de seguridad de la organización.
	5.28	Recolección de evidencia	Garantizar la integridad de las evidencias recolectadas.	APLICA	Facilita investigaciones forenses y cumplimiento legal.
	5.29	Seguridad de la información durante la interrupción	Mantener la seguridad durante interrupciones operativas.	APLICA	Protege equipos contra accesos no autorizados o pérdidas.
	5.30	Preparación de las TIC para la continuidad del negocio	Garantizar que los sistemas TIC soporten la continuidad del negocio.	APLICA	Asegura la protección de activos en ubicaciones externas.
	5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Cumplir con todas las leyes y regulaciones aplicables.	APLICA	Minimiza riesgos en la contratación de personal.
	5.32	Declaraciones de propiedad intelectual	Proteger la propiedad intelectual de la organización.	APLICA	Controla el acceso a información clasificada y crítica.
	5.33	Protección de registros	Asegurar la protección de registros clave.	APLICA	Evita fugas de información tras la desvinculación de empleados.
	5.34	Privacidad y protección de la información identificable de las personas (PII)	Garantizar la protección de datos personales.	APLICA	Evita manipulaciones no autorizadas en el código fuente.
	5.35	Revisión independiente de la seguridad de la información	Realizar auditorías independientes de seguridad.	APLICA	Evita interrupciones en la continuidad del negocio.
	5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	Verificar que se cumplan las políticas establecidas.	APLICA	Elimina la recuperación de datos en equipos descartados.
	5.37	Procedimientos operativos documentados	Documentar procedimientos para la gestión de seguridad.	APLICA	Evita fugas de información tras la desvinculación de empleados.
6. Controles de Personas	6.1	Chequeo	Verificar antecedentes antes de contratar.	APLICA	Minimiza riesgos en la contratación de personal.
	6.2	Términos y condiciones de empleo	Establecer responsabilidades relacionadas con la seguridad en los contratos.	APLICA	Asegura la seguridad física de oficinas y salas de reunión.
	6.3	Concienciación, educación y capacitación en seguridad de la información	Educar a los empleados sobre prácticas seguras.	APLICA	Controla y protege el acceso a infraestructuras sensibles.
	6.4	Proceso disciplinario	Definir acciones ante incumplimientos de seguridad.	APLICA	Garantiza la disponibilidad de la información crítica.
	6.5	Responsabilidades después de la terminación o cambio de empleo	Proteger la información tras cambios laborales.	APLICA	Garantiza que los sistemas de almacenamiento sean confiables.
	6.6	Acuerdos de confidencialidad o de no divulgación	Formalizar acuerdos para proteger información confidencial.	APLICA	Limita accesos privilegiados para evitar abusos de autoridad.
	6.7	Trabajo remoto	Garantizar la seguridad en entornos de trabajo remoto.	APLICA	Evita fugas de información tras la desvinculación de empleados.
	6.8	Informes de eventos de seguridad de la información	Asegurar que los empleados reporten eventos de seguridad.	APLICA	Refuerza los mecanismos de autenticación de usuarios.
7. Controles Físicos	7.1	Perímetro de seguridad física	Establecer barreras físicas para proteger instalaciones.	APLICA	Protege equipos contra accesos no autorizados o pérdidas.
	7.2	Entrada física	Controlar el acceso a instalaciones críticas.	APLICA	Controla y protege el acceso a infraestructuras sensibles.
	7.3	Asegurar oficinas, salas e instalaciones	Proteger las áreas que contienen activos importantes.	APLICA	Evita interrupciones en los sistemas de apoyo operativo.
	7.4	Monitoreo de seguridad física	Implementar vigilancia para detectar amenazas físicas.	APLICA	Permite detectar amenazas físicas en tiempo real.
	7.5	Protección contra amenazas físicas y ambientales	Reducir riesgos por eventos físicos y ambientales.	APLICA	Asegura que el mantenimiento de equipos no comprometa la seguridad.
	7.6	Trabajar en áreas seguras	Asegurar que áreas críticas estén protegidas.	APLICA	Asegura que la información esté protegida en todo momento.
	7.7	Escritorio despejado y pantalla despejada	Prevenir exposición accidental de información.	APLICA	Evita fugas de información tras la desvinculación de empleados.
	7.8	Emplazamiento y protección de equipos	Proteger equipos contra daños o acceso no autorizado.	APLICA	Protege la infraestructura contra sabotajes o fallos físicos.
	7.9	Seguridad de los activos fuera de las instalaciones	Asegurar los activos en ubicaciones externas.	APLICA	Facilita la continuidad de procesos mediante documentación adecuada.
	7.10	Medios de almacenamiento		APLICA	Mantiene configuraciones seguras en los sistemas de la empresa.
	7.11	Utilidades de apoyo	Asegurar que los sistemas de soporte sean confiables.	APLICA	Protege equipos contra accesos no autorizados o pérdidas.
	7.12	Seguridad del cableado	Proteger el cableado contra manipulaciones.	APLICA	Facilita la continuidad de procesos mediante documentación adecuada.
	7.13	Mantenimiento de equipos	Asegurar que el mantenimiento no comprometa la seguridad.	APLICA	Evita exposiciones accidentales de datos sensibles.
	7.14	Eliminación segura o reutilización de equipos	Garantizar que los datos sean eliminados de equipos desechados.	APLICA	Evita exposiciones accidentales de datos sensibles.
8. Controles Tecnológicos	8.1	Dispositivos de punto final de usuario	Proteger los dispositivos utilizados por usuarios finales.	APLICA	Protege equipos contra accesos no autorizados o pérdidas.
	8.2	Derechos de acceso de privilegiado	Limitar accesos con privilegios elevados.	APLICA	Protege dispositivos de usuario contra amenazas cibernéticas.
	8.3	Restricción de acceso a la información	Controlar quién puede acceder a qué información.	APLICA	Permite la identificación de vulnerabilidades mediante auditorías.
	8.4	Acceso al código fuente	Proteger el acceso al código fuente de sistemas.	APLICA	Evita manipulaciones no autorizadas en el código fuente.
	8.5	Autenticación segura	Implementar mecanismos fuertes de autenticación.	APLICA	Protege información sensible mediante acuerdos de confidencialidad.
	8.6	Gestión de capacidad	Proteger contraseñas y otros datos de autenticación.	APLICA	Protege información sensible mediante acuerdos de confidencialidad.
	8.7	Protección contra malware	Usar soluciones para prevenir y detectar malware.	APLICA	Define responsabilidades claras en temas de seguridad.
	8.8	Gestión de vulnerabilidades técnicas	Identificar y corregir vulnerabilidades técnicas.	APLICA	Controla y protege el acceso a infraestructuras sensibles.
	8.9	Gestión de la configuración	Asegurar que los sistemas estén configurados correctamente.	APLICA	Evita interrupciones en la continuidad del negocio.
	8.10	Eliminación de información	Asegurar que los datos sean eliminados de forma segura.	NO APLICA	Previene incidentes de seguridad por incumplimiento de normas.
	8.11	Enmascaramiento de datos	Proteger los datos durante su almacenamiento.	APLICA	Asegura que el mantenimiento de equipos no comprometa la seguridad.
	8.12	Protección de fuga de datos	Implementar medidas para prevenir fugas de información.	APLICA	Facilita la identificación y respuesta ante incidentes de seguridad.
	8.13	Copia de seguridad de la información	Garantizar la recuperación de datos en caso de pérdida.	APLICA	Identifica y corrige vulnerabilidades antes de que sean explotadas.
	8.14	Redundancia de las instalaciones de procesamiento de información	Implementar redundancia para mayor disponibilidad.	APLICA	Previene infecciones por malware y ataques de virus.
	8.15	Inicio sesión	Registrar eventos relevantes en los sistemas.	APLICA	Protege equipos contra accesos no autorizados o pérdidas.
	8.16	Actividades de seguimiento	Monitorear sistemas para detectar anomalías.	APLICA	Garantiza que los sistemas de almacenamiento sean confiables.
	8.17	Sincronización de reloj	Asegurar que los relojes de los sistemas estén sincronizados.	APLICA	Protege dispositivos de usuario contra amenazas cibernéticas.
	8.18	Uso de programas de utilidad privilegiados	Controlar el uso de herramientas con privilegios elevados.	APLICA	Facilita la continuidad de procesos mediante documentación adecuada.
	8.19	Instalación de software en sistemas operativos	Proteger los sistemas operativos de riesgos a la instalación de software.	APLICA	Previene infecciones por malware y ataques de virus.
	8.20	Seguridad de la red	Implementar medidas para proteger redes.	APLICA	Cumple con las regulaciones y normativas aplicables.
	8.21	Seguridad de los servicios de red	Supervisar redes para detectar problemas.	APLICA	Evita manipulaciones no autorizadas en el código fuente.
	8.22	Segregación de redes	Separar redes para limitar el impacto de incidentes.	APLICA	Protege la infraestructura contra sabotajes o fallos físicos.
	8.23	Filtrado web	Categorizar las páginas permitidas en la organización.	APLICA	Restringe el acceso a áreas con información clasificada.
	8.24	Uso de criptografía	Usar criptografía para proteger datos.	APLICA	Previene incidentes de seguridad por incumplimiento de normas.
	8.25	Ciclo de vida de desarrollo seguro	Incorporar seguridad en todas las etapas del desarrollo.	NO APLICA	Asegura que la información esté protegida en todo momento.
	8.26	Requisitos de seguridad de la aplicación	Definir requerimientos de seguridad para aplicaciones.	NO APLICA	Garantiza que los sistemas de almacenamiento sean confiables.
	8.27	Principios de arquitectura e ingeniería de sistemas seguros	Evaluar la arquitectura e ingeniería de sistemas seguros.	NO APLICA	Evita accesos no autorizados a instalaciones críticas.
	8.28	Codificación segura	Asegurar que el código sea desarrollado con buenas prácticas de seguridad.	NO APLICA	Permite la identificación de vulnerabilidades mediante auditorías.
	8.29	Pruebas de seguridad en desarrollo y aceptación	Establecer controles para ambientes de desarrollo y prueba.	NO APLICA	Resguarda los datos personales y la privacidad de los usuarios.
	8.30	Desarrollo subcontratado	Asegurar que proveedores externos sigan prácticas seguras.	NO APLICA	Cumple con las regulaciones y normativas aplicables.
	8.31	Peparación de los entornos de desarrollo, prueba y producción	Implementar medidas para proteger estos entornos.	NO APLICA	Asegura la protección de activos en ubicaciones externas.
	8.32	Gestión del cambio	Gestionar los cambios de manera controlada y segura.	NO APLICA	Evita exposiciones accidentales de datos sensibles.
	8.33	Información de la prueba	Proteger la información utilizada en pruebas.	NO APLICA	Evita manipulaciones no autorizadas en el código fuente.
	8.34	Protección de los sistemas de información durante las pruebas de auditoría	Asegurar que las auditorías no comprometan la seguridad.	NO APLICA	Restringe el acceso a áreas con información clasificada.