FOCUS SYSTEMS PERU SAC
SEPTIEMBRE 2024

DECLARACIÓN DE APLICABILIDAD - REQUISITOS

Número	Requisito	Aplica	Justificación	Método de Implementación
4	**Contexto de la Organización**			
4.1	**Contexto Organizacional**			
4.1	Determinar los objetivos del SGSI de la organización y cualquier cuestión que pueda comprometer su efectividad	Si	Requisito de la norma ISO/IEC 27001: 2022	- Análisis Interno y Externo: Realizar un análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas) para identificar factores que puedan afectar el SGSI. - Revisión Estratégica: Identificar objetivos estratégicos y operativos relacionados con la seguridad de la información.
4.2	**Partes Interesadas**			
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc	Si	Requisito de la norma ISO/IEC 27001: 2022	- Mapa de Partes Interesadas: Crear un mapa que clasifique a las partes interesadas según su influencia e interés (clientes, empleados, proveedores, reguladores). - Consulta Activa: Realizar entrevistas o talleres con stakeholders clave para identificar sus expectativas
4.2 (b)	Determinar sus requisitos relevantes al respecto de la seguridad de la información y sus obligaciones	Si	Requisito de la norma ISO/IEC 27001: 2022	- Revisión Legal y Regulatoria: Analizar las leyes, regulaciones y estándares aplicables al sector (e.g., RGPD, Ley de Protección de Datos). - Revisión Contractual: Identificar cláusulas relacionadas con la seguridad en contratos con proveedores y clientes. - Matriz de Requisitos: Documentar los requisitos identificados en una matriz para su seguimiento.
4.3	**Alcance del SGSI**			

4.3	Determinar y documentar el alcance del SGSI	Si	Requisito de la norma ISO/IEC 27001: 2022	- Definición del Alcance: Identificar procesos, unidades organizativas y ubicaciones físicas y digitales a incluir en el SGSI. - Mapa de Procesos: Elaborar un diagrama de procesos clave. - Declaración Formal: Documentar el alcance en un informe aprobado por la dirección.
4.4	**SGSI**			
4.4	Establecer, implementar, mantener y mejorar continuamente un SGSI de conformidad con la norma	Si	Requisito de la norma ISO/IEC 27001: 2022	- Política de Seguridad: Definir una política de seguridad aprobada por la alta dirección. - Planificación Estratégica: Crear un plan maestro con actividades, cronogramas y responsables. - Ciclo PDCA: Implementar un ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar).
5	**Liderazgo**			
5.1	**Liderazgo y Compromiso**			
5.1	La alta dirección debe demostrar liderazgo y compromiso en relación con el SGSI	Si	Requisito de la norma ISO/IEC 27001: 2022	- Compromiso Formal: Emitir una declaración pública y documentada de compromiso con el SGSI. - Reuniones Periódicas: Organizar reuniones con la alta dirección para revisar avances del SGSI. - Participación Activa: Involucrar a la alta dirección en auditorías y revisiones de políticas.
5.2	**Política**			
5.2	Establecer la política de seguridad de la información	Si	Requisito de la norma ISO/IEC 27001: 2022	- Definición de Política: Redactar una política alineada con los objetivos estratégicos de la organización. - Aprobación por la Dirección: Asegurar que la alta dirección apruebe y comunique la política. - Divulgación Interna: Publicar la política en los canales internos (intranet, reuniones, capacitaciones).
5.3	**Roles, Responsabilidades y Autoridades en la Organización**			

5.3	Asignar y comunicar los roles y responsabilidades de la seguridad de la información	Si	Requisito de la norma ISO/IEC 27001: 2022	- Matriz de Responsabilidades: Crear una matriz RACI (Responsable, Aprobador, Consultado, Informado) para las actividades de seguridad. - Designación Formal: Emitir nombramientos escritos para los responsables del SGSI. - Comunicación: Realizar capacitaciones para informar a los empleados sobre sus roles.
6	**Planificación**			
6.1	**Acciones para Tratar con los Riesgos y Oportunidades**			
6.1.1	Diseñar / planificar el SGSI para satisfacer los requisitos, tratando con los riesgos y oportunidades	Si	Requisito de la norma ISO/IEC 27001: 2022	- Identificación de Riesgos y Oportunidades: Realizar talleres con áreas clave. - Análisis de Contexto: Usar metodologías como PESTEL o SWOT. - Planificación: Diseñar un cronograma con responsables para gestionar los riesgos detectados.
6.1.2	Definir y aplicar un proceso de apreciación de riesgos de seguridad de la información	Si	Requisito de la norma ISO/IEC 27001: 2022	- Metodología Formal: Usar estándares como ISO 31000. - Evaluación de Impacto y Probabilidad: Clasificar los riesgos según matrices cualitativas o cuantitativas. - Documentación: Mantener registros claros en un repositorio centralizado.
6.1.3	Documentar y aplicar un proceso de tratamiento de riesgos de seguridad de la información	Si	Requisito de la norma ISO/IEC 27001: 2022	- Selección de Controles: Basarse en el Anexo A de la norma. - Planes de Mitigación: Diseñar acciones específicas con responsables y fechas. - Seguimiento: Usar indicadores para medir la efectividad del tratamiento implementado.
6.2	**Objetivos y Planes de Seguridad de la Información**			
6.2	Establecer y documentar los objetivos y planes de seguridad de la información	Si	Requisito de la norma ISO/IEC 27001: 2022	- Definición SMART: Asegurar que los objetivos sean específicos, medibles, alcanzables, relevantes y con tiempo definido. - Aprobación Directiva: Involucrar a la alta dirección. - Monitoreo Continuo: Evaluar avances en reuniones periódicas.

6.3	**Planificación de Cambios**			
6.3	Los cambios sustanciales al SGSI deben ser llevados a cabo de manera planificada	Si	Requisito de la norma ISO/IEC 27001: 2022	- Control de Cambios: Establecer un procedimiento basado en ITIL o similar. - Evaluación de Impacto: Realizar un análisis de riesgos previo al cambio. - Comunicación: Informar a las partes interesadas antes de implementar los cambios.
7	**Soporte**			
7.1	**Recursos**			
7.1	Determinar y proporcionar los recursos necesarios para el SGSI	Si	Requisito de la norma ISO/IEC 27001: 2022	- Identificación de Recursos Necesarios: Evaluar necesidades de personal, tecnologías, y presupuestos. - Aprobación Directiva: Presentar un plan detallado a la alta dirección. - Asignación de Recursos: Garantizar la disponibilidad de financiamiento, herramientas y equipos requeridos.
7.2	**Competencias**			
7.2	Determinar, documentar y poner a disposición las competencias necesarias	Si	Requisito de la norma ISO/IEC 27001: 2022	- Análisis de Competencias: Identificar brechas en habilidades relacionadas con seguridad de la información. - Plan de Capacitación: Diseñar un programa formativo basado en normativas como ISO 27001 y requisitos internos. - Certificaciones: Fomentar certificaciones relevantes como CISM, CISSP, o auditor ISO 27001.
7.3	**Concientización**			
7.3	Establecer un programa de concientización en seguridad	Si	Requisito de la norma ISO/IEC 27001: 2022	- Desarrollo de Contenidos: Crear materiales educativos (manuales, videos, etc.) específicos para los riesgos organizacionales. - Campañas Regulares: Realizar capacitaciones trimestrales y ejercicios prácticos como simulaciones de phishing. - Medición del Impacto: Evaluar el nivel de concientización mediante encuestas y métricas.

7.4	**Comunicación**			
7.4	Determinar la necesidad para las comunicaciones internas y externas relevantes al SGSI	Si	Requisito de la norma ISO/IEC 27001: 2022	- Mapa de Comunicación: Identificar quién, cómo y cuándo se comunicará la información relevante del SGSI. - Protocolos de Comunicación Interna: Definir canales como reuniones, correos internos, y plataformas colaborativas. - Externa: Comunicar políticas de seguridad a socios, proveedores y otras partes interesadas según sea necesario.
7.5	**Información Documentada**			
7.5.1	Proveer la documentación requerida por la norma así como la requerida por la organización	Si	Requisito de la norma ISO/IEC 27001: 2022	- Lista Maestra de Documentos: Crear un registro de los documentos requeridos (políticas, procedimientos, registros, etc.). - Cumplimiento Normativo: Asegurarse de incluir todos los elementos mencionados en la norma ISO/IEC 27001:2022. - Sistemas de Gestión Documental: Usar herramientas como SharePoint o Document Control.
7.5.2	Proveer títulos, autores, etc para la documentación, adecuar el formato consistentemente, revisarlos y aprobarlos	Si	Requisito de la norma ISO/IEC 27001: 2022	- Estandarización del Formato: Establecer plantillas oficiales para todos los documentos del SGSI. - Autorización: Definir responsables para la creación y revisión (ej., propietario del documento, revisores, y aprobadores). - Control de Versiones: Utilizar un sistema de versionado claro para cambios en los documentos.
7.5.3	Controlar la documentación adecuadamente	Si	Requisito de la norma ISO/IEC 27001: 2022	- Accesibilidad Controlada: Usar permisos para asegurar que solo las personas autorizadas accedan a ciertos documentos. - Ciclo de Vida del Documento: Implementar políticas para creación, actualización, archivo y eliminación de documentos. - Auditorías Internas: Verificar regularmente el cumplimiento de los controles documentales.
8	**Operación**			

8.1	**Planificación y Control Operacional**			
8.1	Planificar, implementar, controlar y documentar el proceso del SGSI para gestionar los riesgos (i.e. un plan de tratamiento de riesgos)	Si	Requisito de la norma ISO/IEC 27001: 2022	- Planificación del SGSI: Establecer un cronograma y asignar responsabilidades para la gestión de riesgos. - Desarrollo del Plan de Tratamiento: Identificar controles específicos en función de los riesgos detectados. - Monitoreo Operacional: Realizar auditorías regulares para verificar la efectividad.
8.2	**Apreciación del Riesgo de Seguridad de la Información**			
8.2	(Re)hacer la apreciación y documentar los riesgos de seguridad de la información en forma regular y ante cambios o modificaciones	Si	Requisito de la norma ISO/IEC 27001: 2022	- Reevaluación Regular: Implementar un calendario para revisiones periódicas del análisis de riesgos. - Gestión de Cambios: Incorporar la reevaluación de riesgos en el proceso de cambios de TI. - Documentación: Usar herramientas como ISMS.online o Excel para registrar todos los riesgos detectados y actualizados.
8.3	**Tratamiento del Riesgo de Seguridad de la Información**			
8.3	Implementar el plan de tratamiento de riesgos (tratar los riesgos!) y documentar los resultados	Si	Requisito de la norma ISO/IEC 27001: 2022	- Implementación de Controles: Aplicar controles específicos (técnicos, administrativos o físicos) para tratar los riesgos identificados. - Validación del Tratamiento: Realizar pruebas de los controles implementados. - Registro de Resultados: Documentar en un sistema los riesgos mitigados y los pendientes.
9	**Evaluación del Desempeño**			
9.1	**Seguimiento, Medición, Análisis y Evaluación**			

9.1	Hacer seguimiento, medir, analizar y evaluar el SGSI y los controles	Si	Requisito de la norma ISO/IEC 27001: 2022	- Definir Indicadores Clave de Desempeño (KPI): Establecer métricas específicas para evaluar la eficacia de los controles (e.g., incidentes de seguridad, tiempo de respuesta). - Monitoreo Regular: Implementar herramientas de monitoreo como SIEM o dashboards. - Informes: Generar informes regulares para análisis y mejora.
9.2	**Auditoría Interna**			
9.2	Planificar y llevar a cabo auditorias internas del SGSI	Si	Requisito de la norma ISO/IEC 27001: 2022	- Planificación: Crear un plan anual de auditorías internas alineado con el alcance del SGSI. - Ejecución: Designar auditores calificados y llevar a cabo auditorías en base a la norma ISO 19011. - Seguimiento: Documentar hallazgos y realizar acciones correctivas.
9.3	**Revisión por la Dirección**			
9.3	Emprender revisiones por la dirección del SGSI regularmente	Si	Requisito de la norma ISO/IEC 27001: 2022	- Planificación: Agendar revisiones periódicas (al menos una vez al año). - Preparación: Presentar informes sobre resultados de auditorías, métricas de desempeño y mejoras implementadas. - Registro: Documentar las decisiones y acciones acordadas por la alta dirección.
10	**Mejora**			
10.1	**Mejora Continua**			
10.1	Mejorar continuamente el SGSI	Si	Requisito de la norma ISO/IEC 27001: 2022	- Revisión de Desempeño: Utilizar los resultados del seguimiento, medición, auditorías y revisiones por la dirección para identificar áreas de mejora. - Acción Proactiva: Implementar iniciativas de mejora basadas en análisis de tendencias y oportunidades. - Capacitación: Actualizar competencias y conocimiento del personal en seguridad de la información.

10.2	**No Conformidad y Acciones Correctivas**			
10.2	Identificar, corregir y llevar a cabo acciones para prevenir la recurrencia de no conformidades, documentando las acciones	Si	Requisito de la norma ISO/IEC 27001: 2022	- Detección: Implementar un sistema para reportar no conformidades (e.g., una plataforma de tickets o registro centralizado). - Análisis de Causa Raíz: Aplicar herramientas como el diagrama de Ishikawa o los "5 porqués". - Plan de Acción: Definir acciones correctivas y establecer responsables y plazos. - Seguimiento: Verificar la efectividad de las acciones implementadas.

FOCUS SYSTEMS PERU SAC
SEPTIEMBRE 2024

FOCUS business solutions
UNA EMPRESA DE GRUPO DATCO

DECLARACIÓN DE APLICABILIDAD - CONTROLES

Número	Control	Aplica	Justificación	Método de Implementación
5	**Controles Organizativos**			
5.1	Políticas de seguridad de la información	Si	Se deben definir, aprobar por la dirección, publicar y comunicar a personal relevante y partes interesadas las políticas de seguridad de la información y políticas específicas por tema, y revisarlas en intervalos planificados o ante cambios significativos.	Desarrollo de la Política de Seguridad de la Información: - Analizar los requisitos de seguridad de la organización en base a la naturaleza del negocio y los riesgos identificados.
5.2	Funciones y responsabilidades en materia de seguridad de la información	Si	Los roles y responsabilidades en seguridad de la información deben ser definidos y asignados de acuerdo a las necesidades de la organización.	Definición de Roles y Responsabilidades: - Identificar y documentar los roles críticos relacionados con la seguridad de la información (ej. Responsable de Seguridad de la Información, Administradores de TI, Usuarios Clave).
5.3	Segregación de funciones	Si	Deben segregarse las funciones y áreas de responsabilidad en conflicto.	Análisis de Roles y Responsabilidades: - Realizar un análisis de todos los roles y responsabilidades en los procesos de TI, identificando posibles conflictos de interés, áreas de riesgo o falta de control.
5.4	Responsabilidades de la dirección	Si	La dirección debe requerir que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, políticas específicas por tema y procedimientos de la organización.	Definición y Comunicación del Compromiso de la Dirección: - Establecer un compromiso claro por parte de la alta dirección con respecto a la seguridad de la información.
5.5	Contacto con las autoridades	Si	La organización debe establecer y mantener contacto con las autoridades relevantes.	Identificación de Autoridades Relevantes: - Identificar las autoridades regulatorias, agencias gubernamentales y cuerpos legales pertinentes para el sector de TI y la ubicación geográfica de la organización.

5.6	Contacto con grupos de interés especial	Si	La organización debe establecer y mantener contacto con grupos de interés especial o foros de seguridad especializados y asociaciones profesionales.	Identificación de Grupos de Interés: Elaborar un inventario de todos los grupos de interés relevantes para la organización.
5.7	Inteligencia de amenazas	Si	Se debe recopilar y analizar información relacionada con amenazas de seguridad de la información para producir inteligencia de amenazas.	Identificación de Fuentes de Información: Determinar las fuentes confiables de información sobre amenazas y vulnerabilidades (e.g., informes de seguridad, alertas de proveedores, bases de datos de vulnerabilidades).
5.8	Seguridad de la información en la gestión de proyectos	Si	La seguridad de la información debe integrarse en la gestión de proyectos.	Definición de Requisitos de Seguridad: Identificar y documentar los requisitos de seguridad de la información aplicables a cada proyecto desde su inicio.
5.9	Inventario de la información y otros activos asociados	Si	Se debe desarrollar y mantener un inventario de la información y otros activos asociados, incluyendo propietarios.	Identificación de Activos: Identificar todos los activos de información y asociados (hardware, software, datos, documentación, etc.
5.10	Uso aceptable de la información y otros activos asociados	Si	Se deben identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.	Desarrollo de Políticas de Uso: Crear políticas de uso aceptable que definan claramente las normas y restricciones para el uso de información y otros activos (hardware, software, datos).
5.11	Devolución de activos	Si	El personal y otras partes interesadas pertinentes deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.	Desarrollo de Procedimientos de Devolución: Crear procedimientos claros para la devolución de activos de información, que incluyan pasos a seguir cuando los activos sean devueltos o retirados.

5.12	Clasificación de la información	Si	La información debe ser clasificada de acuerdo a las necesidades de seguridad de la información de la organización basadas en la confidencialidad, integridad, disponibilidad y requisitos de partes interesadas relevantes.	Desarrollo de Políticas de Clasificación: Crear y documentar políticas que definan los criterios para clasificar la información en diferentes categorías (e.
5.13	Etiquetado de la información	Si	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por la organización.	Desarrollo de Políticas de Etiquetado: Crear y documentar políticas que especifiquen cómo y cuándo se debe etiquetar la información, incluyendo el formato y contenido de las etiquetas.
5.14	Transferencia de información	Si	Deben existir reglas, procedimientos o acuerdos para todas las instalaciones de transferencia de información dentro de la organización y entre la organización y otras partes.	Desarrollo de Políticas de Transferencia: Crear y documentar políticas que definan los requisitos y procedimientos para la transferencia segura de información, incluyendo métodos de transferencia y controles de seguridad.
5.15	Control de acceso	Si	Se deben establecer e implementar reglas para controlar el acceso físico y lógico a la información y otros activos asociados basados en los requisitos de negocio y de seguridad de la información.	Desarrollo de Políticas de Control de Acceso: Crear y documentar políticas que definan cómo se gestionará el acceso a la información y los sistemas, incluyendo criterios de autorización, métodos de autenticación y revisiones periódicas.
5.16	Gestión de la identidad	Si	Debe gestionarse el ciclo de vida completo de las identidades.	Desarrollo de Políticas de Gestión de Identidades: Crear y documentar políticas que definan los procedimientos para la gestión de identidades, incluyendo la creación, modificación, mantenimiento y eliminación de identidades de usuario.
5.17	Información de autenticación	Si	La asignación y gestión de la información de autenticación debe ser controlada por un proceso de gestión, incluyendo asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	Desarrollo de Políticas de Gestión de Información de Autenticación: Crear y documentar políticas que definan cómo se manejará la información de autenticación, incluyendo el almacenamiento, uso y protección de contraseñas y otros mecanismos de autenticación.

5.18	Derechos de acceso	Si	Los derechos de acceso a la información y otros activos asociados deben ser asignados, revisados, modificados y eliminados de acuerdo con la política específica de la organización y las reglas de control de acceso.	Desarrollo de Políticas de Derechos de Acceso: Crear y documentar políticas que definan cómo se asignarán, revisarán y revocarán los derechos de acceso, basadas en roles, responsabilidades y principios de menor privilegio.
5.19	Seguridad de la información en las relaciones con los proveedores	Si	Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de productos o servicios de proveedores.	Desarrollo de Políticas de Seguridad para Proveedores: Crear y documentar políticas que establezcan los requisitos de seguridad de la información para las relaciones con proveedores, incluyendo la evaluación y gestión de riesgos.
5.20	Gestión de la seguridad de la información en los acuerdos con los proveedores	No	Se deben establecer y acordar con cada proveedor los requisitos relevantes de seguridad de la información basados en el tipo de relación con el proveedor.	Desarrollo de Requisitos de Seguridad en Contratos: Crear y documentar los requisitos de seguridad de la información que deben incluirse en todos los acuerdos con proveedores, tales como protección de datos, requisitos de confidencialidad y procedimientos de notificación de incidentes.
5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Si	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.	Desarrollo de Políticas de Seguridad para la Cadena de Suministro: Crear y documentar políticas que definan los requisitos de seguridad de la información para los proveedores de TIC y para la gestión de la cadena de suministro.
5.22	Monitoreo, revisión y gestión de cambios de los servicios de los proveedores	No	La organización debe monitorear, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información de los proveedores y la entrega de servicios.	Desarrollo de Políticas de Monitoreo y Gestión de Cambios: Crear y documentar políticas que establezcan los requisitos para el monitoreo, revisión y gestión de cambios en los servicios de proveedores, incluyendo la evaluación de impacto en la seguridad de la información.
5.23	Seguridad de la información para el uso de servicios en la nube	Si	Deben establecerse procesos para la adquisición, uso, gestión y salida de servicios en la nube de acuerdo con los requisitos de seguridad de la información de la organización.	Desarrollo de Políticas para Servicios en la Nube: Crear y documentar políticas que definan los requisitos de seguridad específicos para el uso de servicios en la nube, incluyendo controles de acceso, protección de datos y gestión de riesgos.

5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Si	La organización debe planificar y prepararse para gestionar incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos de gestión de incidentes de seguridad de la información, roles y responsabilidades.	Desarrollo de un Plan de Gestión de Incidentes: Crear y documentar un plan de gestión de incidentes que defina los procedimientos para identificar, reportar, evaluar, y responder a los incidentes de seguridad de la información.
5.25	Evaluación y decisión sobre eventos de seguridad de la información	Si	La organización debe evaluar eventos de seguridad de la información y decidir si deben categorizarse como incidentes de seguridad de la información.	Desarrollo de Procedimientos de Evaluación de Eventos: Crear y documentar procedimientos para la evaluación de eventos de seguridad de la información, incluyendo la identificación, clasificación y evaluación del impacto potencial.
5.26	Respuesta a incidentes de seguridad de la información	Si	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Desarrollo de Procedimientos de Respuesta a Incidentes: Crear y documentar procedimientos claros para la respuesta a incidentes de seguridad, especificando los pasos a seguir, las responsabilidades y los recursos necesarios.
5.27	Aprendizaje de los incidentes de seguridad de la información	Si	El conocimiento adquirido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.	Recopilación de Información Post-Incidente: Recolectar toda la información relevante sobre el incidente una vez que se haya resuelto, incluyendo datos sobre el impacto, las causas, las acciones tomadas y los resultados obtenidos.
5.28	Recogida de pruebas	Si	La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.	Desarrollo de Procedimientos de Recolección de Evidencia: Crear y documentar procedimientos para la recolección de evidencia durante y después de un incidente de seguridad, incluyendo métodos para asegurar la integridad y autenticidad de la evidencia.
5.29	Seguridad de la información durante la interrupción	Si	La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.	Desarrollo de Planes de Continuidad de Negocio: Crear y mantener planes de continuidad de negocio que incluyan medidas específicas para proteger la seguridad de la información durante interrupciones, asegurando que se puedan recuperar los servicios y datos críticos.

5.30	Preparación de las TIC para la continuidad del negocio	Si	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse basada en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	Desarrollo de Planes de Continuidad de TIC: Crear y mantener planes específicos para la continuidad de las TIC que detallen cómo se protegerán y recuperarán los sistemas y datos críticos durante una interrupción.
5.31	Identificación de los requisitos legales, reglamentarios y contractuales	Si	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben ser identificados, documentados y mantenidos actualizados.	Identificación de Requisitos Aplicables: Identificar y documentar todos los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información, incluyendo leyes locales, nacionales e internacionales, así como requisitos específicos de contratos con clientes y proveedores.
5.32	Derechos de propiedad intelectual	Si	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.	Identificación de Activos de Propiedad Intelectual: Identificar y documentar todos los activos de propiedad intelectual de la organización, incluyendo patentes, marcas registradas, derechos de autor y secretos comerciales.
5.33	Protección de registros	Si	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.	Identificación de Registros: Identificar y clasificar todos los registros relacionados con la seguridad de la información, incluyendo registros de auditoría, incidentes de seguridad, y resultados de pruebas y evaluaciones.
5.34	Privacidad y protección de la información personal	Si	La organización debe identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de la PII según las leyes y regulaciones aplicables y los requisitos contractuales.	Identificación de PII: Identificar y clasificar toda la información personal identificable (PII) que la organización maneja, incluyendo datos como nombres, direcciones, números de identificación, información financiera y datos de contacto.
5.35	Revisión independiente de la seguridad de la información	Si	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluyendo personas, procesos y tecnologías, debe ser revisado de manera independiente en intervalos planificados, o cuando ocurran cambios significativos.	Planificación de Revisiones Independientes: Definir y programar revisiones independientes periódicas de la seguridad de la información, que pueden incluir auditorías internas, revisiones externas y evaluaciones de terceros.

5.36	Cumplimiento de políticas y normas de seguridad de la información	Si	Se debe revisar regularmente el cumplimiento de la política de seguridad de la información de la organización, políticas específicas, reglas y estándares.	Desarrollo de Políticas y Reglas: Crear y mantener políticas, reglas y estándares claros y actualizados para la seguridad de la información que estén alineados con los requisitos del ISO 27001:2022 y otras normativas aplicables.
5.37	Procedimientos operativos documentados	Si	Los procedimientos operativos para las instalaciones de procesamiento de información deben estar documentados y disponibles para el personal que los necesite.	Identificación de Procedimientos Necesarios: Identificar las operaciones y actividades críticas que requieren procedimientos documentados para gestionar y controlar adecuadamente la seguridad de la información.
6	**Controles de Personas**			
6.1	Selección de personal	No	Se deben realizar verificaciones de antecedentes de todos los candidatos antes de unirse a la organización y de manera continua, considerando las leyes, regulaciones, ética y proporcionalidad a los requisitos del negocio, la clasificación de la información a acceder y los riesgos percibidos.	Definición de Requisitos de Evaluación: Establecer los requisitos y criterios para la evaluación de antecedentes, incluyendo los tipos de antecedentes a revisar (penales, financieros, laborales, etc.
6.2	Términos y condiciones de empleo	No	Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.	Revisión de Políticas y Procedimientos: Revisar y actualizar las políticas y procedimientos de recursos humanos para incluir términos y condiciones relacionados con la seguridad de la información, en conformidad con los requisitos de ISO 27001:2022.
6.3	Concienciación, educación y formación en materia de seguridad de la información	Si	El personal de la organización y las partes interesadas relevantes deben recibir concienciación, educación y capacitación adecuada en seguridad de la información, y actualizaciones regulares de la política de seguridad de la información de la organización, políticas específicas y procedimientos, según sea relevante para su función laboral.	Evaluación de Necesidades de Capacitación: Realizar una evaluación de las necesidades de capacitación en seguridad de la información para identificar los conocimientos y habilidades necesarios para diferentes roles dentro de la organización.
6.4	Proceso disciplinario	Si	Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.	Desarrollo de Políticas Disciplinarias: Crear y documentar una política disciplinaria que detalle las acciones y sanciones en caso de violaciones de las políticas de seguridad de la información.

6.5	Responsabilidades después de la terminación o cambio de empleo	No	Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o cambio de empleo deben definirse, aplicarse y comunicarse al personal y otras partes interesadas relevantes.	Desarrollo de Políticas de Terminación: Crear y documentar políticas que establezcan claramente los procedimientos para la gestión de responsabilidades de seguridad de la información al momento de la terminación o cambio de empleo.
6.6	Acuerdos de confidencialidad o no divulgación	No	Se deben identificar, documentar, revisar regularmente y firmar acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información por parte del personal y otras partes interesadas relevantes.	Desarrollo de Políticas de Confidencialidad: Crear y documentar políticas que establezcan los requisitos y procedimientos para los acuerdos de confidencialidad o no divulgación.
6.7	Trabajo a distancia	Si	Se deben implementar medidas de seguridad cuando el personal trabaje de forma remota para proteger la información accedida, procesada o almacenada fuera de las instalaciones de la organización.	Desarrollo de Políticas de Trabajo Remoto: Crear y documentar políticas que definan los requisitos de seguridad y las prácticas recomendadas para el trabajo remoto.
6.8	Reporte de eventos de seguridad de la información	Si	La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechosos a través de canales apropiados de manera oportuna.	Desarrollo de Procedimientos de Reporte: Crear y documentar procedimientos detallados para el reporte de eventos de seguridad, incluyendo los tipos de eventos que deben ser reportados, los métodos de reporte y los responsables de recibir los reportes.
7	**Controles Físicos**			
7.1	Perímetro de seguridad física	Si	Los perímetros de seguridad deben definirse y utilizarse para proteger áreas que contienen información y otros activos asociados.	Evaluar las áreas críticas: Identificar y mapear las áreas que requieren protección física especial.
7.2	Controles físicos de entrada	Si	Las áreas seguras deben estar protegidas por controles de acceso adecuados y puntos de acceso.	Evaluar las zonas de acceso: Identificar las áreas que requieren controles de acceso físico especial, como salas de servidores, oficinas de alto nivel, etc.

7.3	Seguridad de oficinas, salas e instalaciones	Si	La seguridad física para oficinas, habitaciones e instalaciones debe ser diseñada e implementada.	Realizar un análisis de riesgos: Identificar y evaluar los riesgos asociados con las oficinas, habitaciones e instalaciones para determinar las medidas de seguridad necesarias.
7.4	Supervisión de la seguridad física	Si	Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.	Evaluar las áreas de monitoreo: Identificar las zonas críticas y sensibles que requieren monitoreo continuo, como centros de datos, áreas de almacenamiento de información sensible, etc.
7.5	Protección contra amenazas físicas y ambientales	Si	Se debe diseñar e implementar protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.	Identificar amenazas físicas y ambientales: Realizar un análisis para identificar posibles amenazas físicas (incendios, inundaciones, etc.
7.6	Trabajar en áreas seguras	Si	Las medidas de seguridad para trabajar en áreas seguras deben ser diseñadas e implementadas.	Identificar áreas seguras: Determinar y definir las áreas dentro de las instalaciones que están designadas como seguras para el trabajo con información sensible.
7.7	Escritorio y pantalla despejados	Si	Las reglas de escritorio limpio para papeles y medios de almacenamiento extraíbles y las reglas de pantalla clara para las instalaciones de procesamiento de información deben definirse y aplicarse apropiadamente.	Desarrollar política de escritorio limpio: Crear y documentar una política que exija mantener los escritorios limpios y las pantallas claras de información sensible cuando no están en uso.
7.8	Ubicación y protección de los equipos	Si	Los equipos deben estar ubicados de manera segura y protegidos.	Desarrollar una política de ubicación y protección de equipos: Crear y documentar una política que defina cómo se deben ubicar y proteger los equipos físicos.

7.9	Seguridad de los activos fuera de las instalaciones	Si	Los activos fuera de las instalaciones deben estar protegidos.	Desarrollar una política de seguridad para activos fuera de las instalaciones: Crear y documentar una política específica para la protección de activos cuando se encuentren fuera de las instalaciones de la empresa.
7.10	Medios de almacenamiento	Si	Los medios de almacenamiento deben ser gestionados a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manejo de la organización.	Identificar y clasificar los medios de almacenamiento: Catalogar todos los medios de almacenamiento que contienen información sensible o crítica, como discos duros, cintas, USBs, etc.
7.11	Servicios de apoyo	Si	Las instalaciones de procesamiento de información deben estar protegidas contra fallas de energía y otras interrupciones causadas por fallas en los servicios de soporte.	Evaluar proveedores de servicios de soporte: Realizar una evaluación de seguridad y confiabilidad de los proveedores de servicios de soporte antes de contratar sus servicios.
7.12	Seguridad del cableado	Si	Los cables que transportan energía, datos o servicios de información de soporte deben estar protegidos contra interceptaciones, interferencias o daños.	Identificar y documentar el cableado: Realizar un inventario del cableado existente en todas las instalaciones y documentar su ubicación y propósito.
7.13	Mantenimiento de equipos	Si	Los equipos deben mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.	Establecer un programa de mantenimiento: Definir un plan de mantenimiento regular para todos los equipos críticos, que incluya mantenimiento preventivo y correctivo.
7.14	Seguridad en la eliminación o reutilización de equipos	Si	Los artículos de equipo que contienen medios de almacenamiento deben ser verificados para asegurarse de que cualquier dato sensible y software con licencia haya sido eliminado o sobrescrito de manera segura antes de su disposición o reutilización.	Desarrollar un procedimiento de eliminación y reutilización: Crear y documentar procedimientos que especifiquen cómo deben ser eliminados o reutilizados los equipos de TI, incluyendo la eliminación segura de datos.
8	**Controles Tecnológicos**			

8.1	Dispositivos de punto final del usuario	Si	La información almacenada, procesada o accesible a través de dispositivos de punto final del usuario debe estar protegida.	Desarrollar políticas de seguridad para dispositivos de punto final: Crear y documentar políticas que establezcan los requisitos de seguridad para dispositivos de punto final, como computadoras, teléfonos móviles y tablets.
8.2	Derechos de acceso con privilegios	Si	La asignación y el uso de derechos de acceso privilegiado deben ser restringidos y gestionados.	Identificar y clasificar los accesos privilegiados: Enumerar todos los accesos privilegiados necesarios para la administración y operación de sistemas críticos y clasificar su importancia y riesgo.
8.3	Restricción de acceso a la información	Si	El acceso a la información y otros activos asociados debe ser restringido de acuerdo con la política específica del tema sobre control de acceso.	Identificar y clasificar la información: Catalogar la información según su clasificación y sensibilidad para determinar el nivel de acceso necesario.
8.4	Acceso al código fuente	No	El acceso de lectura y escritura al código fuente, herramientas de desarrollo y bibliotecas de software debe ser gestionado adecuadamente.	Identificar y clasificar el código fuente: Catalogar y clasificar el código fuente según su sensibilidad y el nivel de acceso requerido para garantizar una adecuada protección.
8.5	Autenticación segura	Si	Se deben implementar tecnologías y procedimientos de autenticación segura basados en restricciones de acceso a la información y la política específica del tema sobre control de acceso.	Evaluar los requisitos de autenticación: Identificar y documentar los requisitos de autenticación para diferentes sistemas y aplicaciones en función de los riesgos asociados y el nivel de acceso requerido.
8.6	Gestión de la capacidad	Si	El uso de recursos debe ser monitoreado y ajustado según los requisitos actuales y esperados de capacidad.	Evaluar las necesidades de capacidad: Realizar un análisis para identificar las necesidades actuales y futuras de capacidad basadas en las demandas de negocio y tendencias de crecimiento.

8.7	Protección contra el malware	Si	Se debe implementar protección contra malware, respaldada por la concienciación adecuada de los usuarios.	Evaluar riesgos de malware: Realizar una evaluación de riesgos para identificar las amenazas de malware y determinar las medidas de protección necesarias.
8.8	Gestión de las vulnerabilidades técnicas	Si	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización a estas vulnerabilidades y tomar las medidas adecuadas.	Establecer un proceso de gestión de vulnerabilidades: Definir y documentar un proceso para la identificación, evaluación, y mitigación de vulnerabilidades técnicas en sistemas y aplicaciones.
8.9	Gestión de la configuración	Si	Las configuraciones, incluyendo las de seguridad, de hardware, software, servicios y redes deben ser establecidas, documentadas, implementadas, monitoreadas y revisadas.	Establecer un proceso de gestión de la configuración: Definir y documentar un proceso para la gestión de configuraciones que incluya la identificación, control, y seguimiento de los cambios en los sistemas y aplicaciones.
8.10	Eliminación de información	Si	La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.	Desarrollar políticas de eliminación de información: Definir y documentar políticas y procedimientos para la eliminación segura de información, asegurando que se cumplan los requisitos legales, reglamentarios y contractuales.
8.11	Enmascaramiento de datos	Si	El enmascaramiento de datos debe usarse de acuerdo con la política específica del tema sobre control de acceso y otras políticas relacionadas, y los requisitos del negocio, tomando en consideración la legislación aplicable.	Identificar datos sensibles: Determinar qué datos requieren enmascaramiento, tales como información personal identificable (PII), datos financieros y otra información confidencial.
8.12	Prevención de la fuga de datos	Si	Se deben aplicar medidas de prevención de fuga de datos a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	Evaluar el riesgo de fuga de datos: Realizar una evaluación de riesgos para identificar posibles puntos de fuga de datos y amenazas asociadas.

8.13	Copia de seguridad de la información	Si	Se deben mantener y probar regularmente copias de respaldo de información, software y sistemas de acuerdo con la política específica del tema sobre respaldo.	Identificar datos críticos y esenciales: Determinar qué información debe ser respaldada, incluyendo datos críticos para el negocio, bases de datos y archivos importantes.
8.14	Redundancia de las instalaciones de procesamiento de la información	Si	Las instalaciones de procesamiento de información deben implementarse con redundancia suficiente para satisfacer los requisitos de disponibilidad.	Identificar sistemas críticos: Determinar cuáles sistemas y servicios son críticos para las operaciones de la empresa y requieren redundancia para asegurar la continuidad del negocio.
8.15	Registro de datos	Si	Se deben producir, almacenar, proteger y analizar registros que documenten actividades, excepciones, fallos y otros eventos relevantes.	Identificar tipos de registros necesarios: Determinar qué registros son necesarios para cumplir con los requisitos del sistema de gestión de seguridad de la información (SGSI), incluyendo eventos de seguridad, auditorías, etc.
8.16	Actividades de supervisión	Si	Las redes, sistemas y aplicaciones deben ser monitoreados en busca de comportamientos anómalos y se deben tomar las acciones adecuadas para evaluar posibles incidentes de seguridad de la información.	Definir objetivos de monitoreo: Establecer qué actividades y eventos deben ser monitoreados para cumplir con los objetivos de seguridad de la información.
8.17	Sincronización de relojes	Si	Los relojes de los sistemas de procesamiento de información utilizados por la organización deben ser sincronizados con fuentes de tiempo aprobadas.	Definir políticas de sincronización de tiempo: Establecer directrices y políticas para la sincronización de relojes en todos los sistemas y dispositivos de la organización.
8.18	Uso de programas de utilidad privilegiados	Si	El uso de programas utilitarios que puedan ser capaces de anular los controles de sistemas y aplicaciones debe ser restringido y estrictamente controlado.	Identificar programas utilitarios privilegiados: Realizar un inventario de todos los programas utilitarios que requieren privilegios elevados para su uso.

8.19	Instalación de software en sistemas operativos	Si	Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de software en sistemas operativos.	Definir políticas de instalación de software: Establecer políticas y procedimientos claros para la instalación de software en sistemas operativos, especificando quién está autorizado para realizar estas instalaciones y bajo qué condiciones.
8.20	Controles de red	Si	Las redes y los dispositivos de red deben ser seguros, gestionados y controlados para proteger la información en sistemas y aplicaciones.	Desarrollar políticas de seguridad de red: Establecer políticas que definan cómo se deben proteger las redes, especificando controles y medidas de seguridad necesarios.
8.21	Seguridad de los servicios de red	Si	Se deben identificar, implementar y monitorear mecanismos de seguridad, niveles de servicio y requisitos de servicio de servicios de red.	Evaluar los servicios de red utilizados: Identificar y clasificar todos los servicios de red y comunicación en uso para determinar los riesgos asociados.
8.22	Segregación en redes	Si	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.	Identificar las redes a segregar: Determinar las redes críticas y los segmentos que requieren protección adicional basándose en la clasificación de información y los riesgos asociados.
8.23	Filtrado web	Si	El acceso a sitios web externos debe ser gestionado para reducir la exposición a contenido malicioso.	Evaluar necesidades y objetivos: Identificar los objetivos de seguridad y las necesidades específicas de filtrado web, como prevenir el acceso a sitios web maliciosos o inadecuados.
8.24	Uso de criptografía	Si	Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluyendo la gestión de claves criptográficas.	Evaluar requisitos de criptografía: Identificar los requisitos de criptografía basados en la sensibilidad de la información y los requisitos legales o normativos aplicables.

8.25	Ciclo de vida de desarrollo seguro	No	Se deben establecer y aplicar reglas para el desarrollo seguro de software y sistemas.	Definir requisitos de seguridad: Establecer requisitos de seguridad para el software basado en riesgos y amenazas identificadas, y asegurar que estos requisitos sean incluidos en las especificaciones del proyecto.
8.26	Requisitos de seguridad de las aplicaciones	Si	Los requisitos de seguridad de la información deben ser identificados, especificados y aprobados al desarrollar o adquirir aplicaciones.	Identificar requisitos de seguridad: Realizar un análisis de riesgos para identificar y documentar los requisitos de seguridad específicos para las aplicaciones en función de su uso y el impacto potencial en la seguridad.
8.27	Arquitectura de sistemas seguros y principios de ingeniería	Si	Se deben establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información.	Definir principios de seguridad: Establecer y documentar principios de seguridad que deben ser seguidos en el diseño y la arquitectura de sistemas.
8.28	Codificación segura	No	Se deben aplicar principios de codificación segura en el desarrollo de software.	Desarrollar directrices de codificación segura: Crear y documentar directrices y estándares para la codificación segura que deben ser seguidos por el equipo de desarrollo.
8.29	Pruebas de seguridad en el desarrollo y la aceptación	No	Se deben definir e implementar procesos de pruebas de seguridad en el ciclo de vida de desarrollo.	Definir los requisitos de pruebas de seguridad: Establecer los criterios y objetivos de las pruebas de seguridad en función de los requisitos del sistema y los riesgos identificados.
8.30	Desarrollo externalizado	No	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas externalizado.	Evaluar y seleccionar proveedores: Realizar una evaluación de seguridad y cumplimiento de proveedores que ofrecen servicios de desarrollo externalizado.

8.31	Separación de los entornos de desarrollo, prueba y producción	No	Los entornos de desarrollo, prueba y producción deben estar separados y asegurados.	Definir entornos separados: Establecer y documentar los entornos de desarrollo, prueba y producción como entornos separados, con políticas y procedimientos específicos para cada uno.
8.32	Gestión del cambio	Si	Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.	Desarrollar una política de gestión de cambios: Crear y documentar una política que defina el proceso para la gestión de cambios, incluyendo la planificación, autorización, implementación y revisión de cambios.
8.33	Información de pruebas	No	La información de prueba debe ser seleccionada, protegida y gestionada adecuadamente.	Desarrollar una política para la gestión de información de pruebas: Crear y documentar una política que establezca cómo se debe manejar, almacenar y proteger la información de pruebas.
8.34	Protección de los sistemas de información durante la auditoría y las pruebas	No	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de sistemas operativos deben ser planificadas y acordadas entre el evaluador y la gerencia apropiada.	Desarrollar una política de protección durante pruebas de auditoría: Crear y documentar directrices sobre cómo proteger los sistemas de información y los datos durante las auditorías.

FOCUS SYSTEMS PERU SAC
SEPTIEMBRE 2024

DECLARACIÓN DE APLICABILIDAD - RESUMEN

REQUISITOS

Aplica	4. Contexto	5. Liderazgo	6. Planificación	7. Soporte	8. Operación	9. Evaluación	10. Mejora	Total
Si	5	3	5	7	3	3	2	**28**
No	0	0	0	0	0	0	0	**0**
Total	**5**	**3**	**5**	**7**	**3**	**3**	**2**	**28**

CONTROLES

Aplica	5. Organizacionales	6. Personas	7. Físicos	8. Tecnológicos	Total
Si	35	4	14	26	**79**
No	2	4	0	8	**14**
Total	**37**	**8**	**14**	**34**	**93**