DECLARACIÓN DE APLICABILIDAD (SoA)

Información del Documento

- **Organización:** vvv
- **Fecha de Creación:** 15 de marzo de 2025
- **Versión:** 1.0

1. Introducción

Este documento constituye la Declaración de Aplicabilidad (SoA) para el Sistema de Gestión de Seguridad de la Información (SGSI) de vvv, identificando los controles aplicables de acuerdo con el Anexo A de la norma ISO/IEC 27001:2013.

2. Objetivo

Los objetivos de este documento son:

- Identificar los controles de seguridad aplicables a vvv
- Justificar la inclusión o exclusión de los controles del Anexo A de ISO 27001:2013
- Documentar el estado de implementación de cada control aplicable
- Servir como referencia para la implementación y mejora del SGSI

3. Metodología

La selección de controles se ha realizado considerando:

- Los resultados de la evaluación de riesgos
- Los requisitos legales, regulatorios y contractuales aplicables
- Las prácticas de la industria
- Los objetivos de negocio y de seguridad de la información

4. Leyenda

Aplicabilidad:

- **Aplica:** El control es aplicable y debe ser implementado
- **No Aplica:** El control no es aplicable debido a la naturaleza del negocio o del alcance del SGSI

Estado de Implementación:

- **Implementado:** El control está completamente implementado
- **Parcialmente Implementado:** El control está parcialmente implementado
- **Planificado:** El control está planificado para implementación futura
- **No Implementado:** El control no está implementado

5. Declaración de Aplicabilidad

ID	Control	Aplicabilidad	Estado	Justificación
A.5.1.1	Políticas para la seguridad de la información	Aplica	Parcialmente Implementado	Necesario para proporcionar dirección y apoyo

				para la seguridad de la información
A.5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	Planificado	Necesario para mantener la idoneidad y eficacia de las políticas
A.6.1.1	Roles y responsabilidades de seguridad	Aplica	Implementado	Necesario para establecer un marco de gestión claro
A.6.1.2	Segregación de funciones	Aplica	Parcialmente Implementado	Necesario para prevenir actividades no autorizadas
A.6.1.3	Contacto con las autoridades	Aplica	Implementado	Necesario para cumplimiento legal y gestión de incidentes
A.6.1.4	Contacto con grupos de interés especial	Aplica	No Implementado	Necesario para mantenerse actualizado en seguridad
A.6.1.5	Seguridad de la información en la gestión de proyectos	Aplica	Parcialmente Implementado	Necesario para integrar seguridad desde el diseño
A.6.2.1	Política de dispositivos móviles	Aplica	Planificado	Se utilizan dispositivos móviles para acceder a información corporativa
A.6.2.2	Teletrabajo	Aplica	Parcialmente Implementado	La organización permite el teletrabajo
A.7.1.1	Investigación de antecedentes	Aplica	Implementado	Necesario para verificar candidatos a empleo
A.7.1.2	Términos y condiciones de empleo	Aplica	Implementado	Necesario para establecer responsabilidades de seguridad
A.7.2.1	Responsabilidades de la dirección	Aplica	Parcialmente Implementado	Necesario para asegurar cumplimiento de políticas
A.7.2.2	Concienciación, educación y	Aplica	Planificado	Necesario para asegurar

	capacitación en seguridad de la información			conocimiento de responsabilidades
A.7.2.3	Proceso disciplinario	Aplica	Implementado	Necesario para tratar incumplimientos de seguridad
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Aplica	Implementado	Necesario para proteger intereses durante cambios de personal
A.8.1.1	Inventario de activos	Aplica	Parcialmente Implementado	Necesario para identificar activos que requieren protección
A.8.1.2	Propiedad de los activos	Aplica	Implementado	Necesario para asignar responsabilidad de los activos
A.8.1.3	Uso aceptable de los activos	Aplica	Implementado	Necesario para establecer reglas de uso de activos
A.8.1.4	Devolución de activos	Aplica	Implementado	Necesario para recuperar activos al terminar empleo
A.8.2.1	Clasificación de la información	Aplica	Parcialmente Implementado	Necesario para asegurar protección adecuada
A.8.2.2	Etiquetado de la información	Aplica	Planificado	Necesario para facilitar el manejo de información
A.8.2.3	Manipulación de activos	Aplica	Parcialmente Implementado	Necesario para prevenir divulgación no autorizada
A.8.3.1	Gestión de medios removibles	Aplica	Parcialmente Implementado	Se utilizan medios removibles en la organización
A.8.3.2	Eliminación de medios	Aplica	Implementado	Necesario para prevenir divulgación no autorizada
A.8.3.3	Transferencia de medios físicos	Aplica	Implementado	Necesario para prevenir acceso no

				autorizado durante transporte
A.9.1.1	Política de control de acceso	Aplica	Implementado	Necesario para limitar acceso a información
A.9.1.2	Acceso a redes y servicios de red	Aplica	Implementado	Necesario para prevenir acceso no autorizado a redes
A.9.2.1	Registro y baja de usuarios	Aplica	Implementado	Necesario para asegurar acceso autorizado
A.9.2.2	Provisión de acceso de usuarios	Aplica	Implementado	Necesario para asignar derechos de acceso
A.9.2.3	Gestión de privilegios de acceso	Aplica	Parcialmente Implementado	Necesario para controlar asignación de privilegios
A.9.2.4	Gestión de información secreta de autenticación de usuarios	Aplica	Implementado	Necesario para asegurar contraseñas y credenciales
A.9.2.5	Revisión de derechos de acceso de usuarios	Aplica	Planificado	Necesario para mantener control de acceso actualizado
A.9.2.6	Retiro o ajuste de derechos de acceso	Aplica	Implementado	Necesario cuando cambia el estado de los usuarios
A.9.4.1	Restricción de acceso a la información	Aplica	Implementado	Necesario para prevenir acceso no autorizado
A.18.1.1	Identificación de legislación aplicable y requisitos contractuales	Aplica	Implementado	Necesario para cumplimiento legal y contractual
A.18.1.2	Derechos de propiedad intelectual	Aplica	Implementado	Necesario para proteger propiedad intelectual
A.18.1.3	Protección de registros	Aplica	Parcialmente Implementado	Necesario para prevenir pérdida o falsificación
A.18.1.4	Privacidad y protección de datos	Aplica	Implementado	Necesario para cumplir con RGPD y

	personales			otras leyes
A.18.1.5	Regulación de controles criptográficos	Aplica	Parcialmente Implementado	Necesario para cumplir con regulaciones
A.18.2.1	Revisión independiente de la seguridad de la información	Aplica	Planificado	Necesario para verificar implementación adecuada
A.18.2.2	Cumplimiento de políticas y normas de seguridad	Aplica	Parcialmente Implementado	Necesario para verificar cumplimiento interno
A.18.2.3	Verificación del cumplimiento técnico	Aplica	Planificado	Necesario para verificar configuraciones

6. Controles Excluidos

No hay controles excluidos. Todos los controles del Anexo A de ISO 27001:2013 son aplicables a la organización.

7. Conclusiones

Esta Declaración de Aplicabilidad será revisada y actualizada:

- Al menos una vez al año
- Después de cambios significativos en la organización
- Después de revisiones de la evaluación de riesgos
- Después de incidentes de seguridad significativos

8. Aprobación

Aprobado por: Nombre: _____ Cargo: _____ Fecha: _____ Firma: _____