FOCUS SYSTEMS PERU SAC
SEPTIEMBRE 2024

FOCUS business solutions
UNA EMPRESA DE GRUPO DATCO

ANÁLISIS DE BRECHAS - REQUISITOS

Número	Control	Estado	Evidencia
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	0. No Cumple	
4.2	**Partes Interesadas**		
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc	0. No Cumple	
4.2 (b)	Determinar sus requisitos relevantes al respecto de la seguridad de la información y sus obligaciones	0. No Cumple	
4.3	**Alcance del SGSI**		
4.3	Determinar y documentar el alcance del SGSI	0. No Cumple	
4.4	**SGSI**		
4.4	Establecer, implementar, mantener y mejorar continuamente un SGSI de conformidad con la norma	0. No Cumple	
5	**Liderazgo**		
5.1	**Liderazgo y Compromiso**		
5.1	La alta dirección debe demostrar liderazgo y compromiso en relación con el SGSI	0. No Cumple	
5.2	**Política**		
5.2	Establecer la política de seguridad de la información	0. No Cumple	
5.3	**Roles, Responsabilidades y Autoridades en la Organización**		
5.3	Asignar y comunicar los roles y responsabilidades de la seguridad de la información	0. No Cumple	
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	0. No Cumple	
6.1.2	Definir y aplicar un proceso de apreciación de riesgos de seguridad de la información	0. No Cumple	
6.1.3	Documentar y aplicar un proceso de tratamiento de riesgos de seguridad de la información	0. No Cumple	
6.2	**Objetivos y Planes de Seguridad de la Información**		
6.2	Establecer y documentar los objetivos y planes de seguridad de la información	0. No Cumple	
6.3	**Planificación de Cambios**		
6.3	Los cambios sustanciales al SGSI deben ser llevados a cabo de manera planificada	0. No Cumple	
7	**Soporte**		

7.1	**Recursos**		
7.1	Determinar y proporcionar los recursos necesarios para el SGSI	0. No Cumple	
7.2	**Competencias**		
7.2	Determinar, documentar y poner a disposición las competencias necesarias	0. No Cumple	
7.3	**Concientización**		
7.3	Establecer un programa de concientización en seguridad	0. No Cumple	
7.4	**Comunicación**		
7.4	Determinar la necesidad para las comunicaciones internas y externas relevantes al SGSI	0. No Cumple	
7.5	**Información Documentada**		
7.5.1	Proveer la documentación requerida por la norma así como la requerida por la organización	0. No Cumple	
7.5.2	Proveer títulos, autores, etc para la documentación, adecuar el formato consistentemente, revisarlos y aprobarlos	0. No Cumple	
7.5.3	Controlar la documentación adecuadamente	0. No Cumple	
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)	0. No Cumple	
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	0. No Cumple	
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	0. No Cumple	
9	**Evaluación del Desempeño**		
9.1	**Seguimiento, Medición, Análisis y Evaluación**		
9.1	Hacer seguimiento, medir, analizar y evaluar el SGSI y los controles	0. No Cumple	
9.2	**Auditoría Interna**		
9.2	Planificar y llevar a cabo auditorias internas del SGSI	0. No Cumple	
9.3	**Revisión por la Dirección**		
9.3	Emprender revisiones por la dirección del SGSI regularmente	0. No Cumple	
10	**Mejora**		
10.1	**Mejora Continua**		
10.1	Mejorar continuamente el SGSI	0. No Cumple	

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	0. No Cumple	

FOCUS SYSTEMS PERU SAC
SEPTIEMBRE 2024

FOCUS business solutions
UNA EMPRESA DE GRUPO DATCO

ANÁLISIS DE BRECHAS - CONTROLES

Número	Control	Estado	Evidencia
5	**Controles Organizacionales**		
5.1	Políticas de seguridad de la información	0. No Cumple	
5.2	Funciones y responsabilidades en materia de seguridad de la información	0. No Cumple	
5.3	Segregación de funciones	0. No Cumple	
5.4	Responsabilidades de la dirección	0. No Cumple	
5.5	Contacto con las autoridades	0. No Cumple	
5.6	Contacto con grupos de interés especial	0. No Cumple	
5.7	Inteligencia de amenazas	0. No Cumple	
5.8	Seguridad de la información en la gestión de proyectos	0. No Cumple	
5.9	Inventario de la información y otros activos asociados	0. No Cumple	
5.10	Uso aceptable de la información y otros activos asociados	0. No Cumple	
5.11	Devolución de activos	0. No Cumple	
5.12	Clasificación de la información	0. No Cumple	
5.13	Etiquetado de la información	0. No Cumple	
5.14	Transferencia de información	0. No Cumple	
5.15	Control de acceso	0. No Cumple	
5.16	Gestión de la identidad	0. No Cumple	
5.17	Información de autenticación	0. No Cumple	
5.18	Derechos de acceso	0. No Cumple	
5.19	Seguridad de la información en las relaciones con los proveedores	0. No Cumple	
5.20	Gestión de la seguridad de la información en los acuerdos con los proveedores	No Aplica	
5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	0. No Cumple	
5.22	Monitoreo, revisión y gestión de cambios de los servicios de los proveedores	No Aplica	
5.23	Seguridad de la información para el uso de servicios en la nube	0. No Cumple	
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	0. No Cumple	
5.25	Evaluación y decisión sobre eventos de seguridad de la información	0. No Cumple	
5.26	Respuesta a incidentes de seguridad de la información	0. No Cumple	

5.27	Aprendizaje de los incidentes de seguridad de la información	0. No Cumple	
5.28	Recogida de pruebas	0. No Cumple	
5.29	Seguridad de la información durante la interrupción	0. No Cumple	
5.30	Preparación de las TIC para la continuidad del negocio	0. No Cumple	
5.31	Identificación de los requisitos legales, reglamentarios y contractuales	0. No Cumple	
5.32	Derechos de propiedad intelectual	0. No Cumple	
5.33	Protección de registros	0. No Cumple	
5.34	Privacidad y protección de la información personal	0. No Cumple	
5.35	Revisión independiente de la seguridad de la información	0. No Cumple	
5.36	Cumplimiento de políticas y normas de seguridad de la información	0. No Cumple	
5.37	Procedimientos operativos documentados	0. No Cumple	
6	**Controles de Personas**		
6.1	Selección de personal	No Aplica	
6.2	Términos y condiciones de empleo	No Aplica	
6.3	Concienciación, educación y formación en materia de seguridad de la información	0. No Cumple	
6.4	Proceso disciplinario	0. No Cumple	
6.5	Responsabilidades después de la terminación o cambio de empleo	No Aplica	
6.6	Acuerdos de confidencialidad o no divulgación	No Aplica	
6.7	Trabajo a distancia	0. No Cumple	
6.8	Reporte de eventos de seguridad de la información	0. No Cumple	
7	**Controles Físicos**		
7.1	Perímetro de seguridad física	0. No Cumple	
7.2	Controles físicos de entrada	0. No Cumple	
7.3	Seguridad de oficinas, salas e instalaciones	0. No Cumple	
7.4	Supervisión de la seguridad física	0. No Cumple	
7.5	Protección contra amenazas físicas y ambientales	0. No Cumple	
7.6	Trabajar en áreas seguras	0. No Cumple	
7.7	Escritorio y pantalla despejados	0. No Cumple	
7.8	Ubicación y protección de los equipos	0. No Cumple	
7.9	Seguridad de los activos fuera de las instalaciones	0. No Cumple	

7.10	Medios de almacenamiento	0. No Cumple	
7.11	Servicios de apoyo	0. No Cumple	
7.12	Seguridad del cableado	0. No Cumple	
7.13	Mantenimiento de equipos	0. No Cumple	
7.14	Seguridad en la eliminación o reutilización de equipos	0. No Cumple	
8	**Controles Tecnológicos**		
8.1	Dispositivos de punto final del usuario	0. No Cumple	
8.2	Derechos de acceso con privilegios	0. No Cumple	
8.3	Restricción de acceso a la información	0. No Cumple	
8.4	Acceso al código fuente	No Aplica	
8.5	Autenticación segura	0. No Cumple	
8.6	Gestión de la capacidad	0. No Cumple	
8.7	Protección contra el malware	0. No Cumple	
8.8	Gestión de las vulnerabilidades técnicas	0. No Cumple	
8.9	Gestión de la configuración	0. No Cumple	
8.10	Eliminación de información	0. No Cumple	
8.11	Enmascaramiento de datos	0. No Cumple	
8.12	Prevención de la fuga de datos	0. No Cumple	
8.13	Copia de seguridad de la información	0. No Cumple	
8.14	Redundancia de las instalaciones de procesamiento de la información	0. No Cumple	
8.15	Registro de datos	0. No Cumple	
8.16	Actividades de supervisión	0. No Cumple	
8.17	Sincronización de relojes	0. No Cumple	
8.18	Uso de programas de utilidad privilegiados	0. No Cumple	
8.19	Instalación de software en sistemas operativos	0. No Cumple	
8.20	Controles de red	0. No Cumple	
8.21	Seguridad de los servicios de red	0. No Cumple	
8.22	Segregación en redes	0. No Cumple	
8.23	Filtrado web	0. No Cumple	
8.24	Uso de criptografía	0. No Cumple	

8.25	Ciclo de vida de desarrollo seguro	No Aplica	
8.26	Requisitos de seguridad de las aplicaciones	0. No Cumple	
8.27	Arquitectura de sistemas seguros y principios de ingeniería	0. No Cumple	
8.28	Codificación segura	No Aplica	
8.29	Pruebas de seguridad en el desarrollo y la aceptación	No Aplica	
8.30	Desarrollo externalizado	No Aplica	
8.31	Separación de los entornos de desarrollo, prueba y producción	No Aplica	
8.32	Gestión del cambio	0. No Cumple	
8.33	Información de pruebas	No Aplica	
8.34	Protección de los sistemas de información durante la auditoría y las pruebas	No Aplica	

FOCUS SYSTEMS PERU SAC
SEPTIEMBRE 2024

ANÁLISIS DE BRECHAS - RESUMEN

REQUISITOS

Estado		4. Contexto	5. Liderazgo	6. Planificación	7. Soporte	8. Operación	9. Evaluación	10. Mejora	Total
No Aplica	El control no es aplicable para la entidad.	0	0	0	0	0	0	0	**0**
0. No Cumple	No existe o no se esta haciendo.	5	3	5	7	3	3	2	**28**
1. Inicial	Se hace pero no esta documentado.	0	0	0	0	0	0	0	**0**
2. Limitado	Se hace y esta documentado.	0	0	0	0	0	0	0	**0**
3. Definido	Se hace, esta documentado y se difunde.	0	0	0	0	0	0	0	**0**
4. Gestionado	Se hace, esta documentado, se difunde y se recopilan métricas.	0	0	0	0	0	0	0	**0**
5. Optimizado	Se hace, esta documentado, se difunde, se recopilan métricas y se aplican mejoras de forma continua.	0	0	0	0	0	0	0	**0**
	Total	**5**	**3**	**5**	**7**	**3**	**3**	**2**	**28**

CONTROLES

Estado		5. Organizacionales	6. Personas	7. Físicos	8. Tecnológicos	Total
No Aplica	El control no es aplicable para la entidad.	2	4	0	8	**14**
0. No Cumple	No existe o no se esta haciendo.	35	4	14	26	**79**
1. Inicial	Se hace pero no esta documentado.	0	0	0	0	**0**
2. Limitado	Se hace y esta documentado.	0	0	0	0	**0**
3. Definido	Se hace, esta documentado y se difunde.	0	0	0	0	**0**
4. Gestionado	Se hace, esta documentado, se difunde y se recopilan métricas.	0	0	0	0	**0**
5. Optimizado	Se hace, esta documentado, se difunde, se recopilan métricas y se aplican mejoras de forma continua.	0	0	0	0	**0**
	Total	**37**	**8**	**14**	**34**	**93**