Cuáutitlan Izcalli, miercoles 14 de diciembre de 2022

CONFORMIDAD DE LOS SERVICIOS EN LA APLICABILIDAD DE LA NORMA 27001/2013

A QUIEN CORRESPONDA
PRESENTE.

Por medio de la presente, hacemos contar que el **Sr. Acevedo Andrade Luis Enrique,** la **Srta. Olivares Vega Ana Jesús** y la **Srta. Olvera Mendoza Viridiana,** dieron seguimiento para implementar la norma ISO 27001/2013 en la empresa *ODEKA Creative Workshop S.A. de C.V*, alcanzado lo planificado y obteniendo las metas establecidas. Iniciando su labor a principios de septiembre 2022 hasta la primera semana de diciembre del 2022.

Su desempeño como analistas para determinar los procesos y las políticas más favorables para la empresa fueron excelentes, al igual que su compromiso para implementar dicha norma.

Sin más por el momento agradezco su atención.

ATENTAMENTE

ING. ALEXIS NATERA ARTEAGA
JEFE DE DEPARTAMENTO DE DISEÑO Y PRODUCCIÓN
CEL. 55-5953-2682
CORREO: alexis.natera.art@gmail.com

	Organización

CHECK LIST DE VERIFICACIÓN ISO 27001:2013

* El presente check list tiene como finalidad la verificación del cumplimiento de la Norma ISO 27001:2013

I. Datos de Auditoría.

Nombre del Auditor / Grupo auditor: Acevedo Andrade Luis Enrique	**N° de referencia:**
Lugar de la auditoría: ODEKA S.A DE C.V	**Fecha:** 20/11/2022

II. Requisitos Normativo.

4. Contexto de la Organización.

4.1. Conocimiento de la organización y su contexto

N°	Condición	SI	NO
1	¿Se han identificado las cuestiones internas y extenas que son pertinentes al sistema de Gestion?	x	

4.2. Conocimiento de las necesidades y expectativas de las partes interesadas

N°	Condición	SI	NO
2	¿Se han establecido las partes interesadas?	x	
3	¿Se han identicado cuales necesidades o expectativas se convierten en requisitos legales y otros requisitos?	x	

4.3. Determinación del alcance del sistema de seguridad de la información

N°	Condición	SI	NO
4	¿Se han identificado lo s límites y la aplicabilidad del sistema de seguridad?	x	
5	¿Se ha establecido u n alcance?	x	
6	¿Se ha considerado para el alcance las cuestiones in ternas y externas en el alcance?	x	
7	¿Se ha considerado las necesidades y expectativas de las partes interesadas pertinent es?	x	
8	¿Se mantienen el alcance como información documentada?	x	

4.4. Sistema de Gestión de la Seguridad de la Información

N°	Condición	SI	NO
9	¿Se establece, implementa, mantiene y mejora continuamente un sistema de gestión de seguridad de la informacion?	x	

5. iderazgo y compromiso.

5.1. Liderazgo y compromiso.

N°	Condición	SI	NO
10	¿La alta dirección demostra liderazgo y compromiso con respecto al sistema de gestión de seguridad de la informacion?	x	
11	¿La alta dirección ha establecido la politica y objetiv os del SG de la inform acion y que sean com patibles con la dirección estratégica de la organización?	x	
12	¿Se han integrado los requisitos del sistema de gestion de la información en los procesos de negocio?	x	
13	¿Se cuentan con lo s recursos necesarios para el del SG de la inform acion ?	x	
14	¿La alta dirección se asegura de que el SG de la inform acion alcance los resultados previstos?	x	
15	¿La alta dirección apoya a las personas, para contribuir a la eficacia del SG de la in form acion ?	x	
16	¿La alta dirección promueve la mejora contínua?	x	
17	¿Demuestra liderazgo apoyando a las áreas pertienentes?	x	
18	¿Desarrollando una cult ura en la organización para apoyar los resultados previstos del SG de la informacion ?	x	
19	¿Apoya las funciones de la gerencia para demostrar su liderazgo correspondinel a su Área?	x	

5.2. Política

N°	Condición	SI	NO
20	¿La alta dirección ha establecido implementado y mantenido la política de la seguridad de la informacion?	x	
21	¿La política es adecuada para el proposito de la información e incluye los objetivos de seguridad d ela información?	x	
22	¿Incluye un compromiso para cumplir los requisitos aplicables relacionados?	x	
23	¿Incluye un compromiso para la mejora continua del sistema de gestión de la informadón?	x	
24	¿Incluye un compromiso para la consulta y la participación de los trabajadores y/o los representantes de los trabajadores?	x	
25	¿La política de seguridad se mantiene como información documentada?	x	
26	¿La política de seguridad se comunica dentro de la organización?	x	

27	¿La política de la seguridad está disponible para las partes interesadas?	x	

5.3. Funciones, responsabilidades y autoridad de la organización

N°	Condición	SI	NO
28	¿La alta dirección se asegura que las responsabilidades y autoridades para los roles relacionados con la seguridad de la información?	x	
29	¿La alta dirección asigna responsabilidad y autoridad para garantizar que el sitema de gestión de seguridad de la informacion se adapte a los requisitos de la norma?	x	
30	¿La alta dirección asigna responsabilidad y autoridad para informar a la alta dirección sobre el desempeño del sistema de gestión ?	x	

6. Planificacion.

6.1 Acciones para enfrentar riesgos y oportunidades

6.1.1. Generalidades

N°	Condición	SI	NO
20	¿Se ha considerado en la organización los requisitos del contexto, partes interesadas y el alcance del Sistema de Gestión de la información respecto a los riesgos y oportunidades?	x	
21	¿Se incluyen dentro de los riesgos y oportunidades de PAILL los requisitos legales?	x	
22	¿La organización planifica:	x	
23	a) Las acciones destinadas a manejar estos riesgos y oportunidades	x	
24	b) Evalúa la efectividad de éstas acciones	x	

6.1.2. Evaluación de los riesgos de seguridad de la información

N°	Condición	SI	NO
25	¿La organización deline y aplicar el proceso de evaluación de los riesgos de seguridad de la información?	x	
26	¿establece y mantenienе los criterios de los riesgos de seguridad de la información donde incluye los criterios de aceptación del riesgo?	x	
27	¿Identifica y analiza los riesgos de seguridad de la información?	x	
28	¿La organización conserva información documentada de la Evaluacion de riesgos de la seguridad de la información?	x	

6.1.3 Tratamiento de los riesgos de la seguridad de la Información

N°	Condición	SI	NO
29	¿La organización Selecciona las opciones de tratamiento de los riesgos de seguridad de la información, tomando en cuenta los resultados de la evaluación de los riesgos?	x	
30	¿La organización determina todos los controles que son necesarios para implementar la opción u opciones seleccionadas para el tratamiento de la seguridad de la información?	x	
31	¿La organización conserva información documentada del tratamiento de riesgos de seguridad de información por medio de un plan previamente aprobado?	x	

6.2 Objetivos de Seguridad de la Información y la planificación para alcanzarlos

N°	Condición	SI	NO
32	¿Los objetivos de la seguridad de la información?	x	
33	a) son coherentes con la política de la Seguridad de la información?	x	
34	b) toman en cuenta los requisitos de la seguridad de la información y los resultados de la evaluación de riesgos y del tratamiento de riesgos	x	
35	¿La organización cuenta con información documentada de los objetivos de seguridad de la información?	x	

47	¿Se actualiza la información según sea conveniente según lo definido en la organización?	x	
48	¿Se considera en la actualización la información general, los formatos pertinentes y la revisión y aprobación?	x	
49	¿Se controla la información de forma efectiva para que esté disponible y sea idónea?	x	
50	¿Se protege la información para evitar perdida de su integridad?	x	
51	¿Se almacena la información de forma adecuada y se conserva según sea pertinente a lo definido por la organización?	x	
52	¿Se controla la información externa pertinente al sistema de gestión de SI?	x	

7. Apoyo / Soporte.

7.1 Recursos.

N°	Condición	SI	NO
36	¿La organización proporciona los recursos necesarios para la puesta en marcha del SGSI?	x	

7.2. Competencia.

N°	Condición	SI	NO
37	¿Se determina la competencia necesaria para el personal que hace trabajos relacionados la SGSI?	x	
38	¿Se capacita al personal según las necesidades para adquirir las competencias necesarias?	x	
39	¿Se conserva documentación como evidencia de la competencia?	x	

7.3. Concientización.

N°	Condición	SI	NO
40	¿El personal de la organización conoce la política de seguridad de la información?	x	
41	¿El personal es consciente de su contribución al logro de los objetivos de SGSI?	x	
42	¿Se ha tomado conciencia de lo que implican las no conformidades a los requisitos de seguridad de la información?	x	

7.4. Comunicación.

N°	Condición	SI	NO
43	¿Se han determinado las necesidades de comunicación internas y externas de SGSI?	x	
44	¿Se ha definido el proceso de comunicación?	x	
45	¿Se han determinado los elementos necesarios en la comunicación para que esta sea efectiva?	x	

7.5. Documentación de la información.

N°	Condición	SI	NO
46	¿Se ha identificado que información debe documentarse, según los requisitos de la norma y la demás información a documentar pertinente al SGSI?	x	

8. Operación.

8.1 Planificación y control operacional.

N°	Condición	SI	NO
53	¿Se planifican, implementan y controlan los procesos necesarios para cumplir con los requisitos del SGSI?	x	

8.2. Evaluación de los riesgos de seguridad de la información.

N°	Condición	SI	NO
54	¿Se implementan planes para lograr los objetivos de seguridad de la información?	x	
55	¿La organización garantiza la identificación y control de los procesos subcontratados?	x	
56	¿Se realiza evaluación de riesgos a la SI a intervalos planificados o cuando ocurren cambios que afecten al SGSI?	x	

8.3. Tratamiento de los riesgos de la seguridad de la Información.

N°	Condición	SI	NO
57	¿Exise un plan de tratamiento de los riesgos relacionados al SGSI?	x	
58	¿Se conserva información documentada de los requisitos anteriores?	x	

9 Evaluacion de desempeño

9.1 Monitoreo, medicion, analisis y evaluacion

N°	Condición	SI	NO
59	¿Se evalua el desempeño de la segurida de la informacion?	x	
60	¿Se evalua la efectividad del sistema de gestion de la informacion?	x	
61	¿La organización ha determinado las necesidades que deben ser monitoreo y sometidos a medidon?	x	
62	¿Se ha determinado los metodos, medicion, analisis y evaluacion, según corresponda, con la finalidad de garantizar la validez de los resultados?	x	
63	¿Se ha determinadola frecuencia de monitoreo y la medidon?	x	
64	¿Se hadeterminadolael responsable de monitoreo y lamedidon?	x	
65	¿Se hadeterminado la frecuencia de analizar y evaluar los resultados de monitoreo y de la medicion?	x	
66	¿Se hadeterminado el responsable de analizar y evaluar los resultados de monitoreo y de la medidon?	x	
67	¿Se conserva adecuadamente la informacion documentada de la evidencia de los resultados del monitoreo y la medicion?	x	
68	¿Se conserva adecuadamente la informacion documentada de la evidencia de los resultados del monitoreo y la medicion?	x	

9.2 Auditoria Interna

N°	Condición	SI	NO
69	¿La organización ejecuta auditorías internas en intervalos planificados?	x	
70	Las auditorias internas se ajustan a: a) Los propios requisitos de la organización con respecto a su sistema de gestión de la información;	x	
71	Las auditorias internas se ajustan a: a) Los propios requisitos de la organización con respecto a su sistema de gestión de la información; b) Los requisitos de la Norma Internacional	x	
72	¿Las auditoriasse implementan y mantienen de manera efectiva?	x	
73	¿Las auditorias se planifican, establecen, implementan y mantiene un programa o programas, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y reporte?	x	
74	¿Se hadefinido los criterios y alcance de la auditoria?	x	
75	¿Se ha seleccionado auditores y se dirigen auditorías que aseguren la objetividad e imparcialidad del proceso auditor?	x	
76	¿Se hagarantizado que los resultados de la auditoría sean informados a la gerencia correspondiente?	x	
77	¿Se ha conservado información documentada como evidencia del o de los programas y los resultados de la auditoría?	x	

9.3 Revisión de la Dirección

N°	Condición	SI	NO
78	¿La Alta Dirección debe revisar el sistema de gestión de seguridad de la información a intervalos establecidos para garantizar su continua disponibilidad, adecuación y efectividad?	x	