PLANTILLA DE EJEMPLO DE LISTA DE VERIFICACIÓN DE EVALUACIÓN DE RIESGOS DE CIBERSEGURIDAD

CONTROL DE LA ISO 27001	FASES DE IMPLEMENTACIÓN	TAREAS	¿CONFORME?	NOTAS
5	***Políticas de seguridad de la información***			
5.1	**Dirección de gestión para la seguridad de la información**			
5.1.1	Políticas de seguridad de la información	¿Existen políticas de seguridad?	☐	
		¿Todas las políticas están aprobadas por el equipo directivo?	☐	
		¿Prueba del cumplimiento?	☐	
6	***Organización de seguridad de la información***			
6.1	**Roles y responsabilidades de seguridad de la información**			
6.1.1	Roles y responsabilidades de seguridad	¿Se definieron los roles y las responsabilidades?	☐	
6.1.2	Segregación de deberes	¿Se definió la segregación de deberes?	☐	
6.1.3	Contacto con las autoridades	¿Se contactó al organismo/autoridad de verificación para la verificación del cumplimiento?	☐	
6.1.4	Contacto con grupos de interés especiales	¿Se estableció contacto con grupos de interés especiales en relación con el cumplimiento?	☐	
6.1.5	Seguridad de la información en la administración de proyectos	¿Evidencia de la seguridad de la información en la administración de proyectos?	☐	
6.2	**Dispositivos móviles y teletrabajo**			
6.2.1	Política de dispositivos móviles	¿Se definió una política para dispositivos móviles?	☐	
6.2.2	Teletrabajo	¿Se definió una política para trabajar a distancia?	☐	
7	***Seguridad de los recursos humanos***			
7.1	**Antes del empleo**			
7.1.1	Investigación	¿Se definió una política para investigar a los empleados antes del empleo?	☐	
7.1.2	Términos y condiciones de empleo	¿Se definió una política para los términos y las condiciones de empleo de RR. HH.?	☐	
7.2	**Durante el empleo**			
7.2.1	Responsabilidades de administración	¿Se definió una política para las responsabilidades de administración?	☐	
7.2.2	Conocimiento, educación y capacitación de la seguridad de la información	¿Se definió una política para el conocimiento, la educación y la capacitación de la seguridad de la información?	☐	
7.2.3	Proceso disciplinario	¿Se definió una política para el proceso disciplinario en relación con la seguridad de la información?	☐	

7.3	**Despido y cambio de empleo**			
7.3.1	Responsabilidades relativas al despido o al cambio de empleo	¿Se definió una política de RR. HH. para el despido o cambio de empleo en relación con la seguridad de la información?	☐	
8	***Administración de activos***			
8.1	**Responsabilidades por los activos**			
8.1.1	Inventario de activos	¿La lista de inventario de activos está completa?	☐	
8.1.2	Propiedad de los activos	¿La lista de propiedad de los activos está completa?	☐	
8.1.3	Política de uso aceptable de los activos	¿Se definió una política de "uso aceptable" de los activos?	☐	
8.1.4	Devolución de activos	¿Se definió una política de devolución de activos?	☐	
8.2	**Clasificación de la información**			
8.2.1	Clasificación de la información	¿Se definió una política para la clasificación de información?	☐	
8.2.2	Etiquetado de la información	¿Se definió una política para etiquetar la información?	☐	
8.2.3	Gestión de activos	¿Se definió una política para la gestión de activos?	☐	
8.3	**Gestión de medios**			
8.3.1	Administración de medios extraíbles	¿Se definió una política para la administración de medios extraíbles?	☐	
8.3.2	Eliminación de medios	¿Se definió una política para la eliminación de medios?	☐	
8.3.3.	Transferencia de medios físicos	¿Se definió una política para la transferencia de medios?	☐	
9	***Control de acceso***			
9.1	**Responsabilidades por los activos**			
9.1.1	Política de control de acceso	¿Se definió una política de control de acceso?	☐	
9.1.2	Acceso a redes y servicios de red	¿Se definió una política para el acceso a redes y servicios de red?	☐	
9.2	**Responsabilidades por los activos**			
9.2.1	Registro y cancelación de registro de usuarios	¿Se definió una política para el registro y la cancelación del registro de activos del usuario?	☐	
9.2.2	Aprovisionamiento de acceso de usuarios	¿Se definió una política para el aprovisionamiento de acceso de usuarios?	☐	
9.2.3	Administración de derechos de acceso privilegiado	¿Se definió una política para la administración de derechos de acceso privilegiado?	☐	

9.2.4	Administración de la información de autenticación secreta de los usuarios	¿Se definió una política para la administración de la información de autenticación secreta de los usuarios?	☐	
9.2.5	Revisión de los derechos de acceso de los usuarios	¿Se definió una política para la revisión de los derechos de acceso de los usuarios?	☐	
9.2.6	Eliminación o ajuste de los derechos de acceso	¿Se definió una política para la eliminación o el ajuste de los derechos de acceso?	☐	
9.3	**Responsabilidades del usuario**			
9.3.1	Uso de la información de autenticación secreta	¿Se definió una política para el uso de la información de autenticación secreta?	☐	
9.4	**Control de acceso a sistemas y aplicaciones**			
9.4.1	Restricciones de acceso a la información	¿Se definió una política para las restricciones de acceso a la información?	☐	
9.4.2	Procedimientos de inicio de sesión seguros	¿Se definió una política para los procedimientos de inicio de sesión seguros?	☐	
9.4.3	Sistema de administración de contraseñas	¿Se definió una política para los sistemas de administración de contraseñas?	☐	
9.4.4	Uso de programas de utilidad con privilegios	¿Se definió una política para el uso de programas de utilidad con privilegios?	☐	
9.4.5	Control de acceso al código fuente del programa	¿Se definió una política para el control de acceso al código fuente del programa?	☐	
10	***Criptografía***			
10.1	**Controles criptográficos**			
10.1.1	Política sobre el uso de controles criptográficos	¿Se definió una política para el uso de controles criptográficos?	☐	
10.1.2	Administración de claves	¿Se definió una política para la administración de claves?	☐	
11	***Seguridad física y medioambiental***			
11.1	**Áreas seguras**			
11.1.1	Perímetro de seguridad física	¿Se definió una política para el perímetro de seguridad física?	☐	
11.1.2	Controles físicos de entrada	¿Se definió una política para los controles físicos de entrada?	☐	
11.1.3	Seguridad de oficinas, habitaciones e instalaciones	¿Se definió una política para la seguridad de oficinas, habitaciones e instalaciones?	☐	
11.1.4	Protección frente a amenazas externas y medioambientales	¿Se definió una política para la protección frente a amenazas externas y medioambientales?	☐	
11.1.5	Trabajo en áreas seguras	¿Se definió una política para trabajar en áreas seguras?	☐	
11.1.6	Áreas de entrega y carga	¿Se definió una política para las áreas de entrega y carga?	☐	

11.2	**Equipamiento**			
11.2.1	Emplazamiento y protección de equipos	¿Se definió una política para el emplazamiento y la protección de equipos?	☐	
11.2.2	Utilidades de soporte	¿Se definió una política para las utilidades de soporte?	☐	
11.2.3	Seguridad del cableado	¿Se definió una política para la seguridad del cableado?	☐	
11.2.4	Mantenimiento de equipos	¿Se definió una política para el mantenimiento de equipos?	☐	
11.2.5	Eliminación de activos	¿Se definió una política para la eliminación de activos?	☐	
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	¿Se definió una política para la seguridad de los equipos y activos fuera de las instalaciones?	☐	
11.2.7	Eliminación o reutilización segura del equipo	¿Se reutilizó o eliminó el equipo de forma segura?	☐	
11.2.8	Equipos de usuarios desatendidos	¿Se definió una política para equipos de usuarios desatendidos?	☐	
11.2.9	Política de escritorio despejado y pantalla despejada	¿Se definió una política de escritorio despejado y una política de pantalla despejada?	☐	
12	***Seguridad de las operaciones***			
12.1	**Procedimientos y responsabilidades operativos**			
12.1.1	Procedimientos operativos documentados	¿Se definió una política para los procedimientos operativos documentados?	☐	
12.1.2	Administración de cambios	¿Se definió una política para la administración de cambios?	☐	
12.1.3	Administración de capacidades	¿Se definió una política para la administración de capacidades?	☐	
12.1.4	Separación de entornos de desarrollo, pruebas y operaciones	¿Se definió una política para la separación de entornos de desarrollo, pruebas y operaciones?	☐	
12.2	**Protección contra malware**			
12.2.1	Controles contra malware	¿Se definió una política para los controles contra el malware?	☐	
12.3	**Copia de seguridad del sistema**			
12.3.1	Copia de seguridad	¿Se definió una política para hacer copias de seguridad de sistemas?	☐	
12.3.2	Copia de seguridad de la información	¿Se definió una política para la copia de seguridad de la información?	☐	
12.4	**Registro y monitoreo**			
12.4.1	Registro de eventos	¿Se definió una política para el registro de eventos?	☐	

12.4.2	Protección de la información de registro	¿Se definió una política para la protección de la información de registro?	☐	
12.4.3	Registro del administrador y del operador	¿Se definió una política para el registro del administrador y del operador?	☐	
12.4.4	Sincronización de reloj	¿Se definió una política para la sincronización del reloj?	☐	
12.5	**Control de software operativo**			
12.5.1	Instalación de software en sistemas operativos	¿Se definió una política para la instalación de software en sistemas operativos?	☐	
12.6	**Administración de vulnerabilidades técnicas**			
12.6.1	Administración de vulnerabilidades técnicas	¿Se definió una política para la administración de vulnerabilidades técnicas?	☐	
12.6.2	Restricción de la instalación de software	¿Se definió una política para restringir la instalación de software?	☐	
12.7	**Consideraciones de auditoría de sistemas de información**			
12.7.1	Control de auditoría del sistema de información	¿Se definió una política para el control de auditoría del sistema de información?	☐	
13	***Seguridad de las comunicaciones***			
13.1	**Administración de la seguridad de la red**			
13.1.1	Controles de red	¿Se definió una política para los controles de red?	☐	
13.1.2	Seguridad de los servicios de red	¿Se definió una política para la seguridad de los servicios de red?	☐	
13.1.3	Segregación en redes	¿Se definió una política para la segregación en las redes?	☐	
13.2	**Transferencia de información**			
13.2.1	Políticas y procedimientos de transferencia de información	¿Se definió una política para las políticas y los procedimientos de transferencia de información?	☐	
13.2.2	Acuerdos sobre transferencias de información	¿Se definió una política para los acuerdos sobre transferencias de información?	☐	
13.2.3	Mensajería electrónica	¿Se definió una política para la mensajería electrónica?	☐	
13.2.4	Acuerdos de confidencialidad o no divulgación	¿Se definió una política para los acuerdos de confidencialidad o no divulgación?	☐	
13.2.5	Adquisición, desarrollo y mantenimiento de sistemas	¿Se definió una política para la adquisición, el desarrollo y el mantenimiento de sistemas?	☐	
14	***Adquisición, desarrollo y mantenimiento de sistemas***			
14.1	**Requisitos de seguridad de los sistemas de información**			
14.1.1	Análisis y especificación de los requisitos de seguridad de la información	¿Se definió una política para el análisis y la especificación de los requisitos de seguridad de la información?	☐	

14.1.2	Protección de los servicios de aplicaciones en redes públicas	¿Se definió una política para la protección de los servicios de aplicaciones en redes públicas?	☐	
14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Se definió una política para la protección de las transacciones de servicios de aplicaciones?	☐	
14.2	**Seguridad en los procesos de desarrollo y soporte**			
14.2.1	Desarrollo interno	¿Se definió una política para el desarrollo interno?	☐	
15	***Relaciones con proveedores***			
15.1.1	Relaciones con proveedores	¿Se definió una política para las relaciones con los proveedores?	☐	
16	***Administración de incidentes de seguridad de la información***			
16.1.1	Gestión de incidentes de seguridad de la información	¿Se definió una política para la administración de la seguridad de la información?	☐	
17	***Aspectos de la seguridad de la información para la administración de la continuidad del negocio***			
17.1	**Continuidad de la seguridad de la información**			
17.1.1	Continuidad de la seguridad de la información	¿Se definió una política para la continuidad de la seguridad de la información?	☐	
17.2	**Redundancias**			
17.2.1	Redundancias	¿Se definió una política para las redundancias?	☐	
18	***Cumplimiento***			
18.1	**Cumplimiento de los requisitos legales y contractuales**			
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	¿Se definió una política para la identificación de la legislación aplicable y los requisitos contractuales?	☐	
18.1.2	Derechos de propiedad intelectual	¿Se definió una política para los derechos de propiedad intelectual?	☐	
18.1.3	Protección de registros	¿Se definió una política para la protección de registros?	☐	
18.1.4	Privacidad y protección de información personal identificable	¿Se definió una política para la privacidad y protección de información personal identificable?	☐	
18.1.5	Regulación de los controles criptográficos	¿Se definió una política para la regulación de controles criptográficos?	☐	
18.1	**Revisión independiente de la seguridad de la información**			
18.1.1	Cumplimiento de las políticas y los estándares de seguridad	¿Se definió una política para el cumplimiento de las políticas y los estándares de seguridad?	☐	
18.1.2	Revisión del cumplimiento técnico	¿Se definió una política para la revisión del cumplimiento técnico?	☐	

DESCARGO DE RESPONSABILIDAD

Todos los artículos, las plantillas o la información que proporcione Smartsheet en el sitio web son solo de referencia. Si bien nos esforzamos por mantener la información actualizada y correcta, no hacemos declaraciones ni garantías de ningún tipo, explícitas o implícitas, sobre la integridad, precisión, confiabilidad, idoneidad o disponibilidad con respecto al sitio web o la información, los artículos, las plantillas o los gráficos relacionados que figuran en el sitio web. Por lo tanto, cualquier confianza que usted deposite en dicha información es estrictamente bajo su propio riesgo.

Esta plantilla se proporciona solo como ejemplo. Esta plantilla no implica de ninguna manera un asesoramiento legal o de cumplimiento. Los usuarios de esta plantilla deben determinar qué información es necesaria para alcanzar sus objetivos.