**LISTA DE VERIFICACIÓN DE CONTINUIDAD DEL NEGOCIO DE LA ISO 27001**

|  |  |  |  |
| --- | --- | --- | --- |
| **SECCIÓN/CATEGORÍA****DE REQUISITOS** | **EVALUACIÓN** | **¿CONFORME?** | **OBSERVACIONES** |
| ***5. Políticas de seguridad de la información*** |  |  |
| 5.1 | ¿Existen políticas de seguridad? |   |  |
| 5.2 | ¿Todas las políticas están aprobadas por el equipo directivo? |   |  |
| 5.3 | ¿Prueba del cumplimiento? |   |  |
| ***6. Organización de seguridad de la información*** |   |  |
| 6.1 | ¿Se definieron los roles y las responsabilidades? |   |  |
| 6.2 | ¿Se definió la segregación de deberes? |   |  |
| 6.3 | ¿Se contactó al organismo/autoridad de verificación para la verificación del cumplimiento? |   |  |
| 6.4 | ¿Se estableció contacto con grupos de interés especiales en relación con el cumplimiento? |   |  |
| 6.5 | ¿Evidencia de la seguridad de la información en la administración de proyectos? |   |  |
| 6.6 | ¿Se definió una política para trabajar a distancia? |   |  |
| ***7. Seguridad de los recursos humanos*** |   |  |
| 7.1 | ¿Se definió una política para investigar a los empleados antes del empleo? |   |  |
| 7.2 | ¿Se definió una política para los términos y las condiciones de empleo de RR. HH.? |   |  |
| 7.3 | ¿Se definió una política para las responsabilidades de administración? |   |  |
| 7.4 | ¿Se definió una política para el conocimiento, la educación y la capacitación de la seguridad de la información? |   |  |
| 7.5 | ¿Se definió una política para el proceso disciplinario relacionado con la seguridad de la información? |   |  |
| 7.6 | ¿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 | ¿La lista de inventario de activos está completa? |   |  |
| 8.2 | ¿La lista de propiedad de los activos está completa? |   |  |
| 8.3 | ¿Se definió una política de “uso aceptable” de los activos? |   |  |
| 8.4 | ¿Se definió una política de devolución de activos? |   |  |
| 8.5 | ¿Se definió una política para la clasificación de información? |   |  |
| 8.6 | ¿Se definió una política para etiquetar la información? |   |  |
| 8.7 | ¿Se definió una política para el manejo de activos? |   |  |
| 8.8 | ¿Se definió una política para la administración de medios extraíbles? |   |  |
| 8.9 | ¿Se definió una política para la eliminación de medios? |   |  |
| 8.10 | ¿Se definió una política para la transferencia física de medios? |   |  |
| ***9. Control de acceso***  |   |  |
| 9.1 | ¿Se definió una política de control de acceso? |   |  |
| 9.2 | ¿Se definió una política para el acceso a redes y servicios de red? |   |  |
| 9.3 | ¿Se definió una política para el registro y la cancelación del registro de activos del usuario? |   |  |
| 9.4 | ¿Se definió una política para el aprovisionamiento de acceso de usuarios? |   |  |
| 9.5 | ¿Se definió una política para la administración de derechos de acceso privilegiado? |   |  |
| 9.6 | ¿Se definió una política para la administración de información de autenticación secreta de los usuarios? |   |  |
| 9.7 | ¿Se definió una política para la revisión de los derechos de acceso de los usuarios? |   |  |
| 9.8 | ¿Se definió una política para la eliminación o el ajuste de los derechos de acceso? |   |  |
| 9.9 | ¿Se definió una política para el uso de la información de autenticación secreta? |   |  |
| 9.10 | ¿Se definió una política para las restricciones de acceso a la información? |   |  |
| 9.11 | ¿Se definió una política para los procedimientos de inicio de sesión seguros? |   |  |
| 9.12 | ¿Se definió una política para los sistemas de administración de contraseñas? |   |  |
| 9.13 | ¿Se definió una política para el uso de programas de utilidad con privilegios? |   |  |
| 9.14 | ¿Se definió una política para el control de acceso del código fuente del programa? |   |  |
| ***10. Criptografía*** |   |  |
| 10.1 | ¿Se definió una política para el uso de controles criptográficos? |   |  |
| 10.2 | ¿Se definió una política para la administración de claves? |   |  |
| ***11. Seguridad física y medioambiental*** |   |  |
| 11.1 | ¿Se definió una política para el perímetro de seguridad física? |   |  |
| 11.2 | ¿Se definió una política para los controles físicos de entrada? |   |  |
| 11.3 | ¿Se definió una política para la seguridad de oficinas, habitaciones e instalaciones? |   |  |
| 11.4 | ¿Se definió una política para la protección frente a amenazas externas y medioambientales? |   |  |
| 11.5 | ¿Se definió una política para trabajar en áreas seguras? |   |  |
| 11.6 | ¿Se definió una política para las áreas de entrega y carga? |   |  |
| 11.7 | ¿Se definió una política para el emplazamiento y la protección de equipos? |   |  |
| 11.8 | ¿Se definió una política para las utilidades de soporte? |   |  |
| 11.9 | ¿Se definió una política para la seguridad del cableado? |   |  |
| 11.10 | ¿Se definió una política para el mantenimiento de equipos? |   |  |
| 11.11 | ¿Se definió una política para la eliminación de activos? |   |  |
| 11.12 | ¿Se definió una política para la seguridad de los equipos y activos fuera de las instalaciones? |   |  |
| 11.13 | ¿Se reutilizó o eliminó el equipo de forma segura? |   |  |
| 11.14 | ¿Se definió una política para equipos de usuarios desatendidos? |   |  |
| 11.15 | ¿Se definió una política de escritorio despejado y una política de pantalla despejada? |   |  |
| ***12. Seguridad de las operaciones*** |   |  |
| 12.1 | ¿Se definió una política para los procedimientos operativos documentados? |   |  |
| 12.2 | ¿Se definió una política para la administración de cambios? |   |  |
| 12.3 | ¿Se definió una política para la administración de capacidades? |   |  |
| 12.4 | ¿Se definió una política para la separación de entornos de desarrollo, pruebas y operaciones? |   |  |
| 12.5 | ¿Se definió una política para los controles contra el malware? |   |  |
| 12.6 | ¿Se definió una política para hacer copias de seguridad de sistemas? |   |  |
| 12.7 | ¿Se definió una política para la copia de seguridad de la información? |   |  |
| 12.8 | ¿Se definió una política para el registro de eventos? |   |  |
| 12.9 | ¿Se definió una política para la protección de la información de registro? |   |  |
| 12.10 | ¿Se definió una política para el registro del administrador y del operador? |   |  |
| 12.11 | ¿Se definió una política para la sincronización del reloj? |   |  |
| 12.12 | ¿Se definió una política para la instalación de software en sistemas operativos? |   |  |
| 12.13 | ¿Se definió una política para la administración de vulnerabilidades técnicas? |   |  |
| 12.14 | ¿Se definió una política para restringir la instalación de software? |   |  |
| 12.15 | ¿Se definió una política para el control de auditoría del sistema de información? |   |  |
| ***13. Seguridad de las comunicaciones*** |   |  |
| 13.1 | ¿Se definió una política para los controles de red? |   |  |
| 13.2 | ¿Se definió una política para la seguridad de los servicios de red? |   |  |
| 13.3 | ¿Se definió una política para la segregación en las redes? |   |  |
| 13.4 | ¿Se definió una política para las políticas y los procedimientos de transferencia de información? |   |  |
| 13.5 | ¿Se definió una política para los acuerdos sobre transferencias de información? |   |  |
| 13.6 | ¿Se definió una política para la mensajería electrónica? |   |  |
| 13.7 | ¿Se definió una política para los acuerdos de confidencialidad o no divulgación? |   |  |
| 13.8 | ¿Se definió una política para la adquisición, el desarrollo y el mantenimiento de sistemas? |   |  |
| ***14. Adquisición, desarrollo y mantenimiento de sistemas*** |   |  |
| 14.1 | ¿Se definió una política para el análisis y la especificación de los requisitos de seguridad de la información? |   |  |
| 14.2 | ¿Se definió una política para la protección de los servicios de aplicaciones en redes públicas? |   |  |
| 14.3 | ¿Se definió una política para la protección de las transacciones de servicios de aplicaciones? |   |  |
| 14.4 | ¿Se definió una política para el desarrollo interno? |   |  |
| ***15. Relaciones con proveedores*** |   |  |
| 15.1 | ¿Se definió una política para las relaciones con los proveedores? |   |  |
| ***16. Administración de incidentes de seguridad de la información*** |   |  |
| 16.1 | ¿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 | ¿Se definió una política para la continuidad de la seguridad de la información? |   |  |
| 17.2 | ¿Se definió una política para las redundancias? |   |  |
| ***18. Cumplimiento*** |   |   |  |
| 18.1 | ¿Se definió una política para la identificación de la legislación aplicable y los requisitos contractuales? |   |  |
| 18.2 | ¿Se definió una política para los derechos de propiedad intelectual? |   |  |
| 18.3 | ¿Se definió una política para la protección de registros? |   |  |
| 18.4 | ¿Se definió una política para la privacidad y protección de información personal identificable? |   |  |
| 18.5 | ¿Se definió una política para la regulación de controles criptográficos? |   |  |
| 18.6 | ¿Se definió una política para el cumplimiento de las políticas y los estándares de seguridad? |   |  |
| 18.7 | ¿Se definió una política para la revisión del cumplimiento técnico? |   |  |

**RENUNCIA**

Todos los artículos, las plantillas o la información que proporcione Smartsheet en el sitio web son solo de referencia. Mientras 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.