CONTROLES APLICABLES NORMA ISO 27002:2022

5. Controles organizacionales

5.1 Políticas para la seguridad de la información
5.2 Roles y responsabilidades de seguridad de la información
5.3 Segregación de deberes
5.4 Responsabilidades de gestión (la dirección)
5.5 Contacto con las autoridades
5.6 Contacto con grupos de interés especial
5.7 Inteligencia de amenazas
5.8 Seguridad de la información en la gestión de proyectos
5.9 Inventario de información y otros activos asociados
5.10 Uso aceptable de información y otros activos asociados
5.11 Retorno de los activos
5.12 Clasificación de información
5.13 Etiquetado de información
5.14 Transferencia de información
5.15 Control de acceso
5.16 Gestión de identidad
5.17 Información de autenticación
5.18 Derechos de acceso
5.19 Seguridad de la información en las relaciones con los proveedores
5.20 Abordar la seguridad de la información dentro de los acuerdos de proveedores
5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC
5.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores
5.23 Seguridad de la información para el uso de servicios en la nube
5.24 Gestión de incidentes de seguridad de la información Planificación y preparación
5.25 Evaluación y decisión sobre eventos de seguridad de la información
5.26 Respuesta a incidentes de seguridad de la información
5.27 Aprender de los incidentes de seguridad de la información
5.28 Recopilación de evidencia
5.29 Seguridad de la información durante eventos disruptivos
5.30 Preparación para las TIC para la continuidad del negocio
5.31 Requisitos legales, legales, regulatorios y contractuales
5.32 Derechos de propiedad intelectual
5.33 Protección de registros
5.34 Privacidad y protección de PII
5.35 Revisión independiente de la seguridad de la información
5.36 Cumplimiento de las políticas, reglas y estándares para la seguridad de la información
5.37 Procedimientos operativos documentados

6. Controles de personas

8.1 Selección
8.2 Términos y condiciones de empleo
8.3 Conciencia de seguridad, educación y capacitación de la información
8.4 Proceso Disciplinario
8.5 Responsabilidades después de la terminación o cambio de empleo
8.6 Acuerdos de confidencialidad o no divulgación
8.7 Trabajo remoto
8.8 Informes de eventos de seguridad de la información

7. Controles físicos

7.1 Perímetros de seguridad física
7.2 Entrada física
7.3 Asegurar oficinas, habitaciones e instalaciones
7.4 Monitoreo de seguridad física
7.5 Protección contra amenazas físicas y ambientales
7.6 Trabajando en áreas seguras
7.7 Descripción de la pantalla y pantalla clara
7.8 Manejo de equipos y protección
7.9 Seguridad de activos fuera de las instalaciones
7.10 Medios de almacenamiento
7.11 Soporte de servicios públicos
7.12 Cableado de seguridad
7.13 Mantenimiento de equipo
7.14 Eliminación o reutilización segura del equipo

8. Controles tecnológicos

8.9 Dispositivos de punto final del usuario
8.10 Derechos de acceso privilegiados
8.11 Restricción de acceso a la información
8.12 Acceso al código fuente
8.13 Autenticación segura
8.14 Gestión de capacidad
8.15 Protección contra malware
8.16 Gestión de vulnerabilidades técnicas
8.17 Gestión de configuración
8.18 Eliminación de información
8.19 Enmascaramiento de datos
8.20 Prevención de fugas de datos
8.21 Copia de seguridad de la información
8.22 Redundancia de instalaciones de procesamiento de información
8.23 Registro
8.24 Actividades de monitoreo
8.25 Sincronización de reloj
8.26 Uso de programas de utilidad privilegiados
8.27 Instalación de software en sistemas operativos
8.28 Seguridad de las redes
8.29 Seguridad de los servicios de red
8.30 Segregación de redes
8.31 Filtrado web
8.32 Uso de la criptografía
8.33 Ciclo de vida de desarrollo seguro
8.34 Requisitos de seguridad de la aplicación
8.35 Principios de arquitectura e ingeniería de sistema seguro
8.36 Codificación segura
8.37 Pruebas de seguridad en desarrollo y aceptación
8.38 Desarrollo subcontratado
8.39 Separación de entornos de desarrollo, prueba y producción
8.40 Gestión del cambio
8.41 Información de prueba
8.42 Protección de sistemas de información durante las pruebas de auditoría