ANEXO A.1 OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA - ISO 27001

5. Políticas de seguridad de la información
5.1 Directrices de gestión de la seguridad de la información
- 5.1.1 Políticas para la seguridad de la información
- 5.1.2 Revisión de las políticas para la seguridad de la información

6. Organización de la seguridad de la información
6.1 Organización interna
- 6.1.1 Roles y responsabilidades en seguridad de la información
- 6.1.2 Segregación de tareas
- 6.1.3 Contacto con las autoridades
- 6.1.4 Contacto con grupos de interés especial
- 6.1.5 Seguridad de la información en la gestión de proyectos

6.2 Los dispositivos móviles y el teletrabajo
- 6.2.1 Política de dispositivos móviles
- 6.2.2 Teletrabajo

7. Seguridad relativa a los recursos humanos
7.1 Antes del empleo
- 7.1.1 Investigación de antecedentes
- 7.1.2 Términos y condiciones del empleo

7.2 Durante el empleo
- 7.2.1 Responsabilidades de gestión
- 7.2.2 Concienciación, educación y capacitación en seguridad de la información
- 7.2.3 Proceso disciplinario

7.3 Finalización del empleo o cambio en el puesto de trabajo
- 7.3.1 Responsabilidades ante la finalización o cambio

8. Gestión de activos
8.1 Responsabilidad sobre los activos
- 8.1.1 Inventario de activos
- 8.1.2 Propiedad de los activos
- 8.1.3 Uso aceptable de los activos
- 8.1.4 Devolución de activos

8.2 Clasificación de la información
- 8.2.1 Clasificación de la información
- 8.2.2 Etiquetado de la información
- 8.2.3 Manipulado de la información

8.3 Manipulación de los soportes
- 8.3.1 Gestión de soportes extraíbles
- 8.3.2 Eliminación de soportes
- 8.3.3 Soportes físicos en tránsito

9. Control de acceso
9.1 Requisitos de negocio para el control de acceso
- 9.1.1 Política de control de acceso
- 9.1.2 Acceso a las redes y a los servicios de red

9.2 Gestión de acceso de usuario
- 9.2.1 Registro y baja de usuario
- 9.2.2 Provisión de acceso de usuario
- 9.2.3 Gestión de privilegios de acceso
- 9.2.4 Gestión de la información secreta de autenticación de los usuarios
- 9.2.5 Revisión de los derechos de acceso de usuario
- 9.2.6 Retirada o reasignación de los derechos de acceso

9.3 Responsabilidades del usuario
- 9.3.1 Uso de la información secreta de autenticación

9.4 Control de acceso a sistemas y aplicaciones
- 9.4.1 Restricción del acceso a la información
- 9.4.2 Procedimientos seguros de inicio de sesión
- 9.4.3 Sistema de gestión de contraseñas
- 9.4.4 Uso de utilidades con privilegios del sistema
- 9.4.5 Control de acceso al código fuente de los programas

10. Criptografía
10.1 Controles criptográficos
- 10.1.1 Política de uso de los controles criptográficos
- 10.1.2 Gestión de claves

11. Seguridad física y del entorno
11.1 Áreas seguras
- 11.1.1 Perímetro de seguridad física
- 11.1.2 Controles físicos de entrada
- 11.1.3 Seguridad de oficinas, despachos y recursos
- 11.1.4 Protección contra las amenazas externas y ambientales
- 11.1.5 El trabajo en áreas seguras
- 11.1.6 Áreas de carga y descarga

11.2 Seguridad de los equipos
- 11.2.1 Emplazamiento y protección de equipos
- 11.2.2 Instalaciones de suministro
- 11.2.3 Seguridad del cableado
- 11.2.4 Mantenimiento de los equipos
- 11.2.5 Retirada de materiales propiedad de la empresa
- 11.2.6 Seguridad de los equipos fuera de las instalaciones
- 11.2.7 Reutilización o eliminación segura de equipos
- 11.2.8 Equipo de usuario desatendido
- 11.2.9 Política de puesto de trabajo despejado y pantalla limpia

12. Seguridad de las operaciones
12.1 Procedimientos y responsabilidades operacionales
- 12.1.1 Documentación de procedimientos operacionales
- 12.1.2 Gestión de cambios
- 12.1.3 Gestión de capacidades
- 12.1.4 Separación de los recursos de desarrollo, prueba y operación

12.2 Protección contra el software malicioso (malware)
- 12.2.1 Controles contra el código malicioso
- 12.3 Copias de seguridad
- 12.3.1 Copias de seguridad de la información

12.4 Registros y supervisión
- 12.4.1 Registro de eventos
- 12.4.2 Protección de la información del registro
- 12.4.3 Registros de administración y operación
- 12.4.4 Sincronización del reloj

12.5 Control del software en explotación
- 12.5.1 Instalación del software en explotación

12.6 Gestión de la vulnerabilidad técnica
- 12.6.1 Gestión de las vulnerabilidades técnicas
- 12.6.2 Restricción en la instalación de software

12.7 Consideraciones sobre la auditoria de sistemas de información
- 12.7.1 Controles de auditoría de sistemas de información

13. Seguridad de las comunicaciones
13.1 Gestión de la seguridad de las redes
- 13.1.1 Controles de red
- 13.1.2 Seguridad de los servicios de red
- 13.1.3 Segregación en redes

13.2 Intercambio de información
- 13.2.1 Políticas y procedimientos de intercambio de información
- 13.2.2 Acuerdos de intercambio de información
- 13.2.3 Mensajería electrónica
- 13.2.4 Acuerdos de confidencialidad o no revelación

14. Adquisición, desarrollo y mantenimiento de los sistemas de información
14.1 Requisitos de seguridad en los sistemas de información
- 14.1.1 Análisis de requisitos y especificaciones de seguridad de la información
- 14.1.2 Asegurar los servicios de aplicaciones en redes públicas
- 14.1.3 Protección de las transacciones de servicios de aplicaciones

14.2 Seguridad en el desarrollo y en los procesos de soporte
- 14.2.1 Política de desarrollo seguro
- 14.2.2 Procedimiento de control de cambios en sistemas
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
- 14.2.4 Restricciones a los cambios en los paquetes de software
- 14.2.5 Principios de ingeniería de sistemas seguros
- 14.2.6 Entorno de desarrollo seguro
- 14.2.7 Externalización del desarrollo de software
- 14.2.8 Pruebas funcionales de seguridad de sistemas
- 14.2.9 Pruebas de aceptación de sistemas

14.3 Datos de prueba
- 14.3.1 Protección de los datos de prueba

15. Relación con proveedores
15.1 Seguridad en las relaciones con proveedores
- 15.1.1 Política de seguridad de la información en las relaciones con los proveedores
- 15.1.2 Requisitos de seguridad en contratos con terceros
- 15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones

15.2 Gestión de la provisión de servicios del proveedor
- 15.2.1 Control y revisión de la provisión de servicios del proveedor
- 15.2.2 Gestión de cambios en la provisión del servicio del proveedor

16. Gestión de incidentes de seguridad de la información
16.1 Gestión de incidentes de seguridad de la información y mejoras
- 16.1.1 Responsabilidades y procedimientos
- 16.1.2 Notificación de los eventos de seguridad de la información
- 16.1.3 Notificación de puntos débiles de la seguridad
- 16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
- 16.1.5 Respuesta a incidentes de seguridad de la información
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información
- 16.1.7 Recopilación de evidencias

17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio
17.1 Continuidad de la seguridad de la información
- 17.1.1 Planificación de la continuidad de la seguridad de la información
- 17.1.2 Implementar la continuidad de la seguridad de la información
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

17.2 Redundancias.
- 17.2.1 Disponibilidad de los recursos de tratamiento de la información

18. Cumplimiento
18.1 Cumplimiento de los requisitos legales y contractuales
- 18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
- 18.1.2 Derechos de Propiedad Intelectual (DPI)
- 18.1.3 Protección de los registros de la organización
- 18.1.4 Protección y privacidad de la información de carácter personal
- 18.1.5 Regulación de los controles criptográficos

18.2 Revisiones de la seguridad de la información
- 18.2.1 Revisión independiente de la seguridad de la información
- 18.2.2 Cumplimiento de las políticas y normas de seguridad
- 18.2.3 Comprobación del cumplimiento técnico

CertiProf®

Professional Knowledge