С	ОС	С	código	control
5	1	1	5.1.1	Políticas de seguridad de la información
5	1	2	5.1.2	Revisión de las políticas de seguridad de la información
			6.1.1	Roles y responsabilidades relativas a la seguridad de la información
6	1	2	6.1.2	Separación de tareas
6	1	3	6.1.3	Contacto con las autoridades
6	1	4	6.1.4	Contacto con grupos de especial interés
6	1	5	6.1.5	Seguridad de la información en la gestión de proyectos
6	2	1	6.2.1	Política de dispositivos móviles
			6.2.2	Teletrabajo
7	1	1	7.1.1	Investigación de antecedentes
7	1	2	7.1.2	Términos y condiciones de contratación
7	2	1	7.2.1 7.2.2	Responsabilidades de la Dirección
7	2	2	7.2.2	Concienciación, formación y capacitación en seguridad de la información
			7.2.3	Proceso disciplinario
7	3	1	7.3.1	Terminación o cambio de responsabilidades laborales
8	3	1	8.3.1	Gestión de soportes extraíbles
		: 1	8.3.2	Retirada de soportes
l		: 4	8.3.3	Transferencia de soportes físicos
9	1	1	9.1.1	Política de control de acceso
9	1	2	9.1.2	Acceso a redes y servicios en red
			9.2.1	Altas y bajas de usuarios
9	2	2	9.2.2	Gestión de derechos de acceso de los usuarios
9	2	3	9.2.3	Gestión de derechos de acceso especiales
9	2	4	9.2.4	Gestión de la información secreta de autenticación de usuarios
9	2	5	9.2.5	Revisión de derechos de acceso de usuario
9	2	6	9.2.6	Terminación o revisión de los privilegios de acceso
9	3	1	9.2.6 9.3.1	Uso de la información secreta de autenticación
9	4	1	9.4.1	Restricción del acceso a la información
9	4	2	9.4.2	Procedimientos seguros de inicio de sesión
9	4	3	9.4.3	Gestión de las contraseñas de usuario
9	4	4	9.4.4	Uso de los recursos del sistema con privilegios especiales
9	4	5	9.4.5	Control de acceso al código fuente de los programas

10	1	1	10.1	Controles criptográficos
10	1	2	10.1.1	Política de uso de los controles criptográficos
10	1	3	10.1.2	Gestión de claves
11	1	1	11.1.1	Perímetro de seguridad física
11	1	2	11.1.2	Controles físicos de entrada
11	1	3	11.1.3	Seguridad de oficinas, despachos e instalaciones
11	1	4	11.1.4	Protección contra las amenazas externas y de origen ambiental
l			11.1.5	Trabajo en áreas seguras
	i		11.1.6	Áreas de carga y descarga
L			11.2.1	Emplazamiento y protección de equipos
11	2	2	11.2.2	Instalaciones de suministro
11	2	3	11.2.3	Seguridad del cableado
	i		11.2.4	Mantenimiento de los equipos
I	:		11.2.5	Retirada de materiales propiedad de la empresa
11	2	6	11.2.6	Seguridad de los equipos fuera de las instalaciones
			11.2.7	Reutilización o retirada segura de equipos
11	2	8	11.2.8	Equipo de usuario desatendido
l 11	2	9	11 2 9	Política de puesto de trabajo despejado y pantalla limpia
12	1	1	12.1.1	Documentación de los procedimientos de operación
	i		12.1.2	Gestión de cambios
			12.1.3	Gestión de capacidades
l	:		12.1.4	Separación de los entornos de desarrollo, prueba y operación
12	2	1	12.2	Protección contra el código malicioso
12	2	2	12.2.1	Controles contra el código malicioso
12	3	1	12.3	Copias de seguridad
	.		12.3.1	Copias de seguridad de la información
			12.4	Registro y monitorización
12	4	2	12.4.1 12.4.2	Registro de eventos
				Protección de la información de los registros
			12.4.3	Registros de administración y operación
12	4	5	12.4.4	Sincronización del reloj
12	5	1	12.5	Control del software en explotación
12	5	2	12.5.1	Instalación de software en sistemas operacionales

4 ~ !	_	, 1	10.6	
12			12.6	Gestión de las vulnerabilidades técnicas
		4	12.6.1	Control de las vulnerabilidades técnicas
	. .		12.6.2	Restricciones a la instalación de software
12	7	1	12.7	Consideraciones sobre la auditoría de los sistemas de información
12			12.7.1	Controles de auditoría de los sistemas de información
13	i .		13.1.1	Controles de red
		4	13.1.2	Seguridad de los servicios de red
			13.1.3	Segregación de redes
			13.2.1	Políticas y procedimientos de transferencia de información
13	2	2	13.2.2	Acuerdos de transferencia de información
13	2	3	13.2.3	Mensajería electrónica
13	2	4	13.2.4	Acuerdos de confidencialidad o no divulgación
14	1	1	14.1.1	Análisis y especificación de los requisitos de seguridad
.	: -		14.1.2	Aseguramiento de servicios y aplicaciones en redes públicas
			14.1.3	Protección de las transacciones
14	2	1	14.2.1	Política de desarrollo seguro
14	2	2	14.2.2	Procedimientos de control de cambios en el sistema
14	2	3	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma
			14.2.4	Restricciones a los cambios en los paquetes de software
			14.2.5	Principios para la ingeniería de sistemas seguros
14	2	6	14.2.6	Entorno de desarrollo seguro
14	2	7	14.2.7	Externalización del desarrollo de software
14	2	8	14.2.8	Pruebas de seguridad del sistema
14	2	9	14.2.9	Pruebas de aceptación del sistema
14	3	1	14.3.1	Protección de los datos de prueba
15	1	1	15.1.1	Política de seguridad de la información en las relaciones con proveedores
15	1	2	15.1.2	Tratamiento de la seguridad en contratos con proveedores
15	1	3	15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones
15	2	1	15.2.1	Supervisión y revisión de los servicios prestados por terceros
15	2	2	15.2.2	Gestión del cambio en los servicios prestados por terceros
16	1	1	16.1.1	Responsabilidades y procedimientos
16	1	2	16.1.2	Notificación de eventos de seguridad de la información
			16.1.3	Notificación de puntos débiles de seguridad

16	1	4	16.1.4	Evaluación y decisión respecto de los eventos de seguridad de la información
16	1	5	16.1.5	Respuesta a incidentes de seguridad de la información
16	1	6	16.1.6	Aprendizaje de los incidentes de seguridad de la información
16	1	7	16.1.7	Recopilación de evidencias
17	1	1	17.1.1	Planificar la continuidad de la seguridad de la información
17	1	2	17.1.2	Implementar la continuidad de la seguridad de la información
17			17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información
17	2	1	17.2.1	Disponibilidad de los medios de procesamiento de información
18	1	1	18.1.1	Identificación de legislación aplicable y requisitos contractuales
18	1	2	18.1.2	Derechos de propiedad intelectual (IPR)
18	1	3	18.1.3	Protección de los documentos de la organización
18	1	4	18.1.4	Protección de datos y privacidad de la información de carácter personal
18	1	5	18.1.5	Regulación de los controles criptográficos
18			18.2.1	Revisión independiente de la seguridad de la información
18	2	2	18.2.2	Cumplimiento de las políticas y normas de seguridad
18	2	3	18.2.3	Comprobación del cumplimiento técnico

С	código	control
5	5	Políticas de seguridad de la información
6	6	Organización de la seguridad de la información
7	7	Seguridad ligada a los recursos humanos
8	8	Gestión de activos
9	9	Control de acceso
10	10	Criptografía
11	11	Seguridad física y del entorno
12		Gestión de operaciones
13	13	Seguridad de las comunicaciones
14	14	Adquisición, desarrollo y mantenimiento de los sistemas
15	15	Relaciones con proveedores
16	16	Gestión de incidentes de seguridad de la información
17	17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio
18	18	Cumplimiento

С	ОС	código	Objetivo de control
5		5.1	Dirección de la gestión de la seguridad de la información
6	1	6.1	Organización interna
6	2 1	6.2	Los dispositivos móviles y el teletrabajo
7	1	7.1	Antes del empleo
7	_	1.2	Durante el empleo
7	3	7.3	Finalización del empleo o cambio de puesto de trabajo
8	1	8.1	Responsabilidad sobre los activos
8	2	8.2	Clasificación de la información
8	3	8.3	Manipulación de los soportes
9	1	9.1	Requisitos de negocio para el control de acceso
9	2	9.2 9.3	Gestión del acceso de usuario
9 9 9	3	9.3	Responsabilidades de usuario
9	4	9.4	Control de acceso a sistema y a aplicaciones
10	1	10.1	Controles criptográficos
11		11.1	Áreas seguras
11		11.2	Seguridad de los equipos
12	1	12.1	Procedimientos y responsabilidades operacionales
12		12.2	Protección contra eñ el software malicioso (malware)
12	3	12.3	Copias de seguridad
12		12.4	Registros y supervisión
12		12.5	Control del software en explotación
12		12.6	Gestión de la vulnerabilidad técnica
12	7	12.7	Consideraciones sobre la auditoría de sistemas de información
13	1	13.1	Gestión de la seguridad de las redes
13		13.2	Transferencia de información
14	1	14.1	Requisitos de seguridad en sistemas de información
14	2	14.2	Seguridad en el desarrollo y en los procesos de soporte
14	3	14.3	Datos de prueba
15	1	15.1	Seguridad en las relaciones con proveedores
15	2	15.2	Gestión de provisión de servicios del proveedor
16		16.1	Gestión de incidentes de seguridad de la información y mejoras
17	1	17.1	Continuidad de la seguridad de la información

17 2	2	17.2	Redundancia
18	1	18.1	Cumplimiento de los requisitos legales y contractuales
18 2	2	18.2	Revisiones de seguridad de la información

С	ОС	С	código	control
5	1	1	5.1.1	Políticas para la seguridad de la información
5	1	2	5.1.2	Revisión de las políticas de seguridad de la información
6	1	1	6.1.1	Roles y responsabilidades relativas a la seguridad de la información
6	1	2	5.1.2 6.1.1 6.1.2	Separación de tareas
6	1	3	6.1.3	Contacto con las autoridades
6	1	4	6.1.4	Contacto con grupos de especial interés
			6.1.5	Seguridad de la información en la gestión de proyectos
6	2	1	6.2.1	Política de dispositivos móviles
6	2	2	6.2.2	Teletrabajo
7	1	1	7.1.1	Investigación de antecedentes
7	1	2	7.1.2	Términos y condiciones de contratación
7	2	1	7.2.1	Responsabilidades de la Dirección
7	2	2	7.2.2	Concienciación, formación y capacitación en seguridad de la información
7	2	3	7.2.3	Proceso disciplinario
1 7	3	1	7.3.1	Terminación o cambio de responsabilidades laborales
8	1	1	8.1.1	Inventario de activos
1			8.1.2	Propiedad de los activos
1	<u></u>		8.1.3	Uso aceptable de los activos
8	1	4	8.1.4	Devolución de activos
8	2	1	8.2.1	Clasificación de la información
8	2	2	8.2.2	Marcado de la información
8	2	3	8.2.2 8.2.3	Manejo de activos
8	3	1	8.3.1	Gestión de soportes extraíbles
8	3	2	8.3.2	Retirada de soportes
1			8.3.3	Transferencia de soportes físicos
			9.1.1	Política de control de acceso
			9.1.2	Acceso a redes y servicios en red
9	2	1	9.2.1	Altas y bajas de usuarios
1 9	2	2	9.2.2	Gestión de derechos de acceso de los usuarios
9	2	3	9.2.3	Gestión de derechos de acceso especiales
9	2	4	9.2.3 9.2.4	Gestión de la información secreta de autenticación de usuarios
9	2	5	9.2.5	Revisión de derechos de acceso de usuario

9 3 1 9.3.1 Uso de la información secreta de autenticación 9 4 1 9.4.1 Restricción del acceso a la información 9 4 2 9.4.2 Procedimientos seguros de inicio de sesión 9 4 3 9.4.3 Gestión de las contraseñas de usuario 9 4 4 9.4.4 Uso de los recursos del sistema con privilegios especiales 9 4 5 9.4.5 Control de acceso al código fuente de los programas 10 1 1 10.1 Controles criptográficos 10 1 2 10.1.1 Política de uso de los controles criptográficos 10 1 3 10.1.2 Gestión de claves 11 1 1 11.1.1 Perímetro de seguridad física 11 1 2 11.1.2 Controles físicos de entrada 11 1 3 11.1.3 Seguridad de oficinas, despachos e instalaciones 11 1 4 11.1.4 Protección contra las amenazas externas y de origen ambiental 11 1 5 11.1.5 Trabajo en áreas seguras 11 1 1 6 11.1.6 Áreas de carga y descarga 11 2 1 11.2.1 Emplazamiento y protección de equipos 11 2 2 11.2.2 Instalaciones de suministro 11 2 3 11.2.3 Seguridad del cableado 11 2 3 11.2.4 Mantenimiento de los equipos 11 2 5 11.2.5 Retirada de materiales propiedad de la empresa 11 2 6 11.2.6 Seguridad de los equipos fuera de las instalaciones 11 2 7 11.2.7 Reutilización o retirada segura de equipos 11 2 8 11.2.8 Equipo de usuario desatendido 11 2 9 11.2.9 Política de puesto de trabajo despejado y pantalla limpia 12 1 1 2.1.1 Documentación de los procedimientos de operación 12 1 1 2 12.1.2 Gestión de cambios 12 1 1 2 12.1.3 Gestión de cambios	_:		ala a c	In the second se
9419.4.1Restricción del acceso a la información9429.4.2Procedimientos seguros de inicio de sesión9439.4.3Gestión de las contraseñas de usuario9449.4.4Uso de los recursos del sistema con privilegios especiales9459.4.5Control de acceso al código fuente de los programas101110.1Controles criptográficos101210.1.1Política de uso de los controles criptográficos101310.1.2Gestión de claves11111.1.1Perímetro de seguridad física111211.1.2Controles físicos de entrada111311.1.3Seguridad de oficinas, despachos e instalaciones111411.1.4Protección contra las amenazas externas y de origen ambiental111511.1.5Trabajo en áreas seguras111611.1.6Áreas de carga y descarga111611.2.1Emplazamiento y protección de equipos112111.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112411.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad del ose equipos fuera de las instalaciones1128 <td< td=""><td></td><td></td><td></td><td>Terminación o revisión de los privilegios de acceso</td></td<>				Terminación o revisión de los privilegios de acceso
9 4 2 9.4.2 Procedimientos seguros de inicio de sesión 9 4 3 9.4.3 Gestión de las contraseñas de usuario 9 4 4 9.4.4 Uso de los recursos del sistema con privilegios especiales 9 4 5 9.4.5 Control de acceso al código fuente de los programas 10 1 1 10.1 Controles criptográficos 10 1 2 10.1.1 Política de uso de los controles criptográficos 10 1 3 10.1.2 Gestión de claves 11 1 1 11.1.1 Perímetro de seguridad física 11 1 2 11.1.2 Controles físicos de entrada 11 1 3 11.1.3 Seguridad de oficinas, despachos e instalaciones 11 1 4 11.1.4 Protección contra las amenazas externas y de origen ambiental 11 1 5 11.1.5 Trabajo en áreas seguras 11 1 6 11.1.6 Áreas de carga y descarga 11 2 1 11.2.1 Emplazamiento y protección de equipos 11 2 2 11.2.2 Instalaciones de suministro 11 2 3 11.2.3 Seguridad del cableado 11 2 4 11.2.4 Mantenimiento de los equipos 11 2 5 11.2.5 Retirada de materiales propiedad de la empresa 11 2 6 11.2.6 Seguridad de los equipos fuera de las instalaciones 11 2 7 11.2.7 Reutilización o retirada segura de equipos 11 2 8 11.2.8 Equipo de usuario desatendido 11 2 9 11.2.9 Política de puesto de trabajo despejado y pantalla limpia 12 1 1 12.1.1 Documentación de los procedimientos de operación 12 1 2 12.1.2 Gestión de cambios 12 1 3 12.1.3 Gestión de cambios				
944/9.4.4Uso de los recursos del sistema con privilegios especiales945/9.4.5Control de acceso al código fuente de los programas1011/10.1Controles criptográficos1012/10.1.1Política de uso de los controles criptográficos1013/10.1.2Gestión de claves1111/11.1.1Perímetro de seguridad física1112/11.1.2Controles físicos de entrada1113/11.1.3Seguridad de oficinas, despachos e instalaciones1114/11.1.4Protección contra las amenazas externas y de origen ambiental1115/11.1.5Trabajo en áreas seguras1116/11.1.6Áreas de carga y descarga112/11.2.1Emplazamiento y protección de equipos112/11.2.2Instalaciones de suministro112/11.2.3Seguridad del cableado112/11.2.4Mantenimiento de los equipos112/5/11.2.5Retirada de materiales propiedad de la empresa112/5/11.2.6Seguridad del os equipos fuera de las instalaciones112/7/11.2.7Reutilización o retirada segura de equipos112/8/11.2.9Política de puesto de trabajo despejado y pantalla limpia121/1/12.1.1Documentación de los procedimientos de operación121/1/12.1.2Gestión de cambios121/1/12.1.3Gestión de cambios				
94494.4Uso de los recursos del sistema con privilegios especiales94594.5Control de acceso al código fuente de los programas101110.1Controles criptográficos101210.1.1Política de uso de los controles criptográficos101310.1.2Gestión de claves11111.1.1Perímetro de seguridad física111211.1.2Controles físicos de entrada111311.1.3Seguridad de oficinas, despachos e instalaciones111411.1.4Protección contra las amenazas externas y de origen ambiental111511.1.5Trabajo en áreas seguras111611.6Áreas de carga y descarga112111.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112311.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación	9	4	2 9.4.2	
94494.4Uso de los recursos del sistema con privilegios especiales94594.5Control de acceso al código fuente de los programas101110.1Controles criptográficos101210.1.1Política de uso de los controles criptográficos101310.1.2Gestión de claves11111.1.1Perímetro de seguridad física111211.1.2Controles físicos de entrada111311.1.3Seguridad de oficinas, despachos e instalaciones111411.1.4Protección contra las amenazas externas y de origen ambiental111511.1.5Trabajo en áreas seguras111611.6Áreas de carga y descarga112111.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112311.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación	9	4	3 9.4.3	Gestión de las contraseñas de usuario
10 1 1 10.1 Controles criptográficos 10 1 2 10.1.1 Política de uso de los controles criptográficos 10 1 3 10.1.2 Gestión de claves 11 1 11.1.1 Perímetro de seguridad física 11 1 2 11.1.2 Controles físicos de entrada 11 1 3 11.1.3 Seguridad de oficinas, despachos e instalaciones 11 1 4 11.1.4 Protección contra las amenazas externas y de origen ambiental 11 1 4 11.1.5 Trabajo en áreas seguras 11 1 6 11.1.6 Áreas de carga y descarga 11 2 1 11.2.1 Emplazamiento y protección de equipos 11 2 1 12.2.2 Instalaciones de suministro 11 2 3 11.2.3 Seguridad del cableado 11 2 4 11.2.4 Mantenimiento de los equipos 11 2 5 11.2.5 <t< td=""><td>9</td><td>4 4</td><td>4 9.4.4</td><td></td></t<>	9	4 4	4 9.4.4	
101210.1.1Política de uso de los controles criptográficos101310.1.2Gestión de claves111111.1.1Perímetro de seguridad física111211.1.2Controles físicos de entrada111311.1.3Seguridad de oficinas, despachos e instalaciones111411.1.4Protección contra las amenazas externas y de origen ambiental111511.1.5Trabajo en áreas seguras111611.1.6Áreas de carga y descarga11211.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112411.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112611.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121121221121122212112222				Control de acceso al código fuente de los programas
10 1 3 10.1.2 Gestión de claves 11 1 11.1.1 Perímetro de seguridad física 11 1 2 11.1.2 Controles físicos de entrada 11 1 3 11.1.3 Seguridad de oficinas, despachos e instalaciones 11 1 4 11.1.4 Protección contra las amenazas externas y de origen ambiental 11 1 5 11.1.5 Trabajo en áreas seguras 11 1 6 11.1.6 Áreas de carga y descarga 11 2 11.2.1 Emplazamiento y protección de equipos 11 2 11.2.2 Instalaciones de suministro 11 2 3 11.2.3 Seguridad del cableado 11 2 4 11.2.4 Mantenimiento de los equipos 11 2 5 11.2.5 Retirada de materiales propiedad de la empresa 11 2 6 11.2.6 Seguridad del los equipos fuera de las instalaciones 11 2 7 11.2.7 Reutili	l			Controles criptográficos
111111.1.1Perímetro de seguridad física111211.1.2Controles físicos de entrada111311.1.3Seguridad de oficinas, despachos e instalaciones111411.1.4Protección contra las amenazas externas y de origen ambiental111511.1.5Trabajo en áreas seguras111611.1.6Áreas de carga y descarga112111.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112311.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112511.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	10	i		Política de uso de los controles criptográficos
111211.1.2Controles físicos de entrada111311.1.3Seguridad de oficinas, despachos e instalaciones111411.1.4Protección contra las amenazas externas y de origen ambiental111511.1.5Trabajo en áreas seguras111611.1.6Áreas de carga y descarga112111.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112311.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112511.2.6Seguridad de los equipos fuera de las instalaciones112611.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	10	1	3 10.1.2	Gestión de claves
111311.1.3Seguridad de oficinas, despachos e instalaciones111411.1.4Protección contra las amenazas externas y de origen ambiental111511.1.5Trabajo en áreas seguras111611.1.6Áreas de carga y descarga112111.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112411.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112511.2.6Seguridad de los equipos fuera de las instalaciones112611.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121212.1.3Gestión de capacidades		i		
111411.1.4Protección contra las amenazas externas y de origen ambiental111511.1.5Trabajo en áreas seguras111611.1.6Áreas de carga y descarga112111.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112411.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112811.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11	1	2 11.1.2	Controles físicos de entrada
11 1 5 11.1.5	11	1	3 11.1.3	Seguridad de oficinas, despachos e instalaciones
11 1 5 11.1.5	11	1	4 11.1.4	Protección contra las amenazas externas y de origen ambiental
112111.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112411.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11;	1 : :	5 11.1.3	Trabajo en áreas seguras
112111.2.1Emplazamiento y protección de equipos112211.2.2Instalaciones de suministro112311.2.3Seguridad del cableado112411.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11	1	6 11.1.6	<u> </u>
112411.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11	2	1 11.2.1	Emplazamiento y protección de equipos
112411.2.4Mantenimiento de los equipos112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11	2	2 11.2.2	
112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades				Seguridad del cableado
112511.2.5Retirada de materiales propiedad de la empresa112611.2.6Seguridad de los equipos fuera de las instalaciones112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11	2	4 11.2.4	Mantenimiento de los equipos
112711.2.7Reutilización o retirada segura de equipos112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11	2	5 11.2.5	
112811.2.8Equipo de usuario desatendido112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11	2	6 11.2.6	Seguridad de los equipos fuera de las instalaciones
112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades				Reutilización o retirada segura de equipos
112911.2.9Política de puesto de trabajo despejado y pantalla limpia121112.1.1Documentación de los procedimientos de operación121212.1.2Gestión de cambios121312.1.3Gestión de capacidades	11	2	8 11.2.8	Equipo de usuario desatendido
12 1 2 12.1.2 Gestión de cambios 12 1 3 12.1.3 Gestión de capacidades	11	2	9 11.2.9	Política de puesto de trabajo despejado y pantalla limpia
12 1 3 12.1.3 Gestión de capacidades	12	1	1 12.1.1	Documentación de los procedimientos de operación
	12	1	2 12.1.2	Gestión de cambios
12: 1: 4 12.1.4 Separación de los entornos de desarrollo, prueba y operación	12			Gestión de capacidades
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	12	1	4 12.1.4	Separación de los entornos de desarrollo, prueba y operación
12 2 1 12.2 Protección contra el código malicioso	12	2	1 12.2	Protección contra el código malicioso
12 2 2 12.2.1 Controles contra el código malicioso	12	2	2 12.2.1	Controles contra el código malicioso
12 3 1 12.3 Copias de seguridad				
12 3 2 12.3.1 Copias de seguridad de la información	12	3	2 12.3.1	Copias de seguridad de la información

12	1	1	12.4	Dogistro vy monitorización
12	4	. <u></u>	12.4	Registro y monitorización
1	4 1		12.4.1	Registro de eventos
		i	12.4.2	Protección de la información de los registros
12	4	4	12.4.3	Registros de administración y operación
			12.4.4	Sincronización del reloj
			12.5	Control del software en explotación
1		:	12.5.1	Instalación de software en sistemas operacionales
12	6	1	12.6	Gestión de las vulnerabilidades técnicas
12	6	2	12.6.1	Control de las vulnerabilidades técnicas
12	ס	3	12.0.2	Restricciones a la instalación de software
12	7	1	12.7	Consideraciones sobre la auditoría de los sistemas de información
12	7	2	12.7.1	Controles de auditoría de los sistemas de información
13	1	1	13.1.1	Controles de red
13	1	2	13.1.2	Seguridad de los servicios de red
13	1	3	13.1.3	Segregación de redes
13	2	1	13.2.1	Políticas y procedimientos de transferencia de información
13	2	2	13.2.2	Acuerdos de transferencia de información
13	2	3	13.2.3	Mensajería electrónica
13	2	4	13.2.3 13.2.4	Acuerdos de confidencialidad o no divulgación
14	1	1	14.1.1	Análisis y especificación de los requisitos de seguridad
14	1	2	14.1.2	Aseguramiento de servicios y aplicaciones en redes públicas
14	1	3	14.1.3	Protección de las transacciones
14	2	1	14.2.1	Política de desarrollo seguro
14	2	2	14.2.2	Procedimientos de control de cambios en el sistema
14	2	3	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma
14	2	4	14 2 4	Restricciones a los cambios en los paquetes de software
14	2	5	14.2.5 14.2.6	Principios para la ingeniería de sistemas seguros
14	2	6	14.2.6	Entorno de desarrollo seguro
14	2	7	14.2.7	Externalización del desarrollo de software
14	2	8	14.2.8	Pruebas de seguridad del sistema
14	2	9	14.2.9	Pruebas de aceptación del sistema
14	3	1	14.3.1	Protección de los datos de prueba
15			15.1.1	Política de seguridad de la información en las relaciones con proveedores
نت		لث		2 charter at argument as in information on instruction of the following

1	2	15.1.2	Tratamiento de la seguridad en contratos con proveedores
1	3	15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones
2	1	15.2.1	Supervisión y revisión de los servicios prestados por terceros
2	2	15.2.2	Gestión del cambio en los servicios prestados por terceros
1	1	16.1.1	Responsabilidades y procedimientos
1	2	16.1.2	Notificación de eventos de seguridad de la información
1	3	16.1.3	Notificación de puntos débiles de seguridad
1	4	16.1.4	Evaluación y decisión respecto de los eventos de seguridad de la información
1	5	16.1.5	Respuesta a incidentes de seguridad de la información
1	6	16.1.6	Aprendizaje de los incidentes de seguridad de la información
1	7	16.1.7	Recopilación de evidencias
1	1	17.1.1	Planificar la continuidad de la seguridad de la información
1	2	17.1.2	Implementar la continuidad de la seguridad de la información
1	3	17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información
2	1	17.2.1	Disponibilidad de los medios de procesamiento de información
1	1	18.1.1	Identificación de legislación aplicable y requisitos contractuales
1	2	18.1.2	Derechos de propiedad intelectual (IPR)
1	3	18.1.3	Protección de los documentos de la organización
1	4	18.1.4	Protección de datos y privacidad de la información de carácter personal
1	5	18.1.5	Regulación de los controles criptográficos
2	1	18.2.1	Revisión independiente de la seguridad de la información
2	2	18.2.2	Cumplimiento de las políticas y normas de seguridad
2	3	18.2.3	Comprobación del cumplimiento técnico
	1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2	1 3 2 1 1 1 2 1 3 1 4 1 1 2 1 3 1 4 1 5 1 5 1 4 1 5 1 2 1 1 2 1 3 1 4 1 5 2 1 1 2 2 2	1 3 15.1.3 2 1 15.2.1 2 2 15.2.2 1 1 16.1.1 1 2 16.1.2 1 3 16.1.3 1 4 16.1.4 1 5 16.1.5 1 6 16.1.6 1 7 16.1.7 1 1 17.1.1 1 2 17.1.2 1 3 17.1.3 2 1 17.2.1 1 1 18.1.1 1 2 18.1.2 1 3 18.1.3 1 4 18.1.4 1 5 18.1.5 2 1 18.2.1 2 2 18.2.2

Nº Trabajo	OC	Objetivo de control de la UNE-ISO/IEC 27002:2015
		o ISO/IEC 27013
1	5.1	Dirección de la gestión de la seguridad de la información
2	6.1	Organización interna
3	6.2	Los dispositivos móviles y el teletrabajo
4	7.1	Antes del empleo
5	7.2	Durante el empleo
6	7.3	Finalización del empleo o cambio de puesto de trabajo
7	8.1	Responsabilidad sobre los activos
8	8.2	Clasificación de la información
9	8.3	Manipulación de los soportes
10	9.1	Requisitos de negocio para el control de acceso
11	9.2	Gestión del acceso de usuario
12	9.3	Responsabilidades de usuario
13	9.4	Control de acceso a sistema y a aplicaciones
14	10.1	Controles criptográficos
15	11.1	Áreas seguras
16	11.2	Seguridad de los equipos
17	12.1	Procedimientos y responsabilidades operacionales
18	12.2	Protección contra el software malicioso (malware)
19	12.3	Copias de seguridad
20	12.4	Registros y supervisión
21	12.5	Control del software en explotación
22	12.6	Gestión de la vulnerabilidad técnica
23	12.7	Consideraciones sobre la auditoría de sistemas de información
24	13.1	Gestión de la seguridad de las redes
25	13.2	Transferencia de información
26	14.1	Requisitos de seguridad en sistemas de información
27	14.2	Seguridad en el desarrollo y en los procesos de soporte
28	14.3	Datos de prueba
29	15.1	Seguridad en las relaciones con proveedores
30	15.2	Gestión de provisión de servicios del proveedor
31	16.1	Gestión de incidentes de seguridad de la información y mejoras

32	17.1	Continuidad de la seguridad de la información
33	17.2	Redundancia
34	18.1	Cumplimiento de los requisitos legales y contractuales
35	18.2	Revisiones de seguridad de la información