IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

ANEXO

ISO 27002: 2022

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

LA NORMA **ISO/IEC 27002** SE CREA BAJO LA COORDINACIÓN DE LA INTERNATIONAL **ORGANIZATION FOR STANDARATION** (**ISO**) Y LA **COMISIÓN ELECTROTÉCNICA INTERNACIONAL** (**IEC**). INICIALMENTE, ERA NORMATIVA **ISO 17799.**

SE ENGLOBA DENTRO DE UN CONJUNTO DE NORMATIVAS **ISO/IEC 2700X** QUE REGULAN TEMAS DE SEGURIDAD EN LOS ÁMBITOS DIGITAL Y ELECTRÓNICO.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ISO 27000

VOCABULARIO QUE SE VA A UTILIZAR EN LAS NORMAS INCLUIDAS EN TODA LA SERIE.

ISO/IEC 27001

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS.

ISO/IEC 27002

GUÍA DE BUENAS PRÁCTICAS QUE DESCRIBE LOS DISTINTOS OBJETIVOS DE CONTROL Y CONTROLES RECOMENDADOS PARA MANTENER UN NIVEL DE SEGURIDAD DE LA INFORMACIÓN ÓPTIMO.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002: 2022

SI BIEN ES CIERTO QUE LA ISO **27002:2013** ESTUVO BIEN ESTRUCTURADA, QUEDÓ LA SENSACIÓN DE QUE **EXISTÍAN MUCHOS DOMINIOS Y CONTROLES** QUE TAL VEZ PODRÍAN SUPLIRSE O AGRUPARSE. ADEMÁS, GENERABAN LA DUDA ACERCA DE SI ESTOS CONTROLES ERAN PREVENTIVOS, DETECTIVOS O REACTIVOS.

LA NUEVA NORMA **ISO 27002:2022**, **INCLUYE UN ENFOQUE PRINCIPALMENTE PREVENTIVO/DETECTIVO** (83 CONTROLES), DE LO QUE SIGNIFICA LA SEGURIDAD DE LA INFORMACIÓN.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002: 2022

LA NORMA ISO **27001:2013**, NOS PRESENTABA **14 DOMINIOS Y 114 CONTROLES**.

LA NORMA ISO **27002:2022** CONTENDRÁ **4 TEMAS Y 93 CONTROLES**.

DOMINIOS ISO 27001:2013	CONTROLES
A.10 Criptografía	2
A.11 Seguridad Física y del Entorno	15
A.12 Seguridad de las Operaciones	14
A.13 Seguridad de las Comunicaciones	7
A.14 Adquisición, desarrollo y mantenimiento de sistemas	13
A.15 Relaciones con los proveedores	5
A.16 Gestión de incidentes de seguridad de la información	7
A.17 Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio	4
A.18 Cumplimiento	8
A.5 Políticas de la Seguridad de la Información	2
A.6 Organización de la seguridad de la información	7
A.7 Seguridad de los Recursos Humanos	6
A.8 Gestión Activos	10
A.9 Control de Acceso	14
Total Controles	**114**

TEMAS ISO 27002:2022	CONTROLES
A.5 Organización	37
A.6 Personas	8
A.7 Objetos Físicos	14
A.8 Tecnología	34
Total Controles	**93**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002: 2022

ISO/IEC 27002 ESTÁ FORMADA POR LAS SECCIONES:

1. ALCANCE
2. REFERENCIAS NORMATIVAS
3. TÉRMINOS, DEFINICIONES Y TÉRMINOS ABREVIADOS
4. ESTRUCTURA DE ESTE DOCUMENTO
5. CONTROLES ORGANIZACIONALES
6. CONTROLES DE PERSONAS
7. CONTROLES FÍSICOS
8. CONTROLES TECNOLÓGICOS

ANEXO A. USANDO ATRIBUTOS

ANEXO B. CORRESPONDENCIA DE ISO/IEC 27002: 2022 CON ISO/IEC 27002:2013

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

1. ALCANCE

ESTE **DOCUMENTO PROPORCIONA UN CONJUNTO DE REFERENCIA DE CONTROLES GENÉRICOS DE SEGURIDAD DE LA INFORMACIÓN, INCLUIDA UNA GUÍA DE IMPLEMENTACIÓN.** ESTE DOCUMENTO **ESTÁ DISEÑADO PARA SER UTILIZADO POR ORGANIZACIONES**:

A. **DENTRO DEL CONTEXTO DE** UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN ISO/IEC 27001;
B. **PARA IMPLEMENTAR CONTROLES** DE SEGURIDAD DE LA INFORMACIÓN **BASADOS EN LAS MEJORES PRÁCTICAS** RECONOCIDAS INTERNACIONALMENTE;
C. **PARA DESARROLLAR DIRECTRICES DE GESTIÓN** DE LA SEGURIDAD DE LA INFORMACIÓN ESPECÍFICAS DE LA ORGANIZACIÓN.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

2. REFERENCIAS NORMATIVAS

NO HAY REFERENCIAS NORMATIVAS EN ESTE DOCUMENTO

3. TÉRMINOS, DEFINICIONES Y TÉRMINOS ABREVIADOS

EXPLICACIÓN DE LOS TÉRMINOS, DEFINICIONES Y TÉRMINOS ABREVIADOS UTILIZADOS EN LA NORMA

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTE DOCUMENTO

4.1 CLÁUSULAS

ESTE DOCUMENTO ESTÁ ESTRUCTURADO DE LA SIGUIENTE MANERA:

a) **CONTROLES ORGANIZACIONALES** (CLÁUSULA 5)

b) **CONTROLES DE PERSONAS** (CLÁUSULA 6)

c) **CONTROLES FÍSICOS** (CLÁUSULA 7)

d) **CONTROLES TECNOLÓGICOS** (CLÁUSULA 8)

HAY **2 ANEXOS INFORMATIVOS**:

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTE DOCUMENTO

4.1 CLÁUSULAS

ANEXO A — USO DE ATRIBUTOS

EXPLICA **CÓMO UNA ORGANIZACIÓN PUEDE USAR ATRIBUTOS PARA CREAR SUS PROPIAS VISTAS** BASADAS EN LOS ATRIBUTOS DE CONTROL DEFINIDOS EN ESTE DOCUMENTO O DE CREACIÓN PROPIA.

CORRESPONDENCIA CON ISO/IEC 27002:2013

MUESTRA LA **CORRESPONDENCIA ENTRE LOS CONTROLES EN ESTA EDICIÓN DE ISO/IEC 27002 Y LA EDICIÓN ANTERIOR DE 2013.**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTE DOCUMENTO

4.2 TEMAS Y ATRIBUTOS

LA CATEGORIZACIÓN DE LOS CONTROLES DADA EN LAS SECCIONES 5 A LA 8 SE DENOMINAN **TEMAS**.

LOS CONTROLES SE CLASIFICAN COMO:

a) **PERSONAS**, SI SE REFIEREN A PERSONAS INDIVIDUALES

b) **FÍSICOS**, SI SE TRATA DE OBJETOS FÍSICOS

c) **TECNOLÓGICOS**, SI SE TRATA DE TECNOLOGÍA

d) EN CASO CONTRARIO SE CATEGORIZAN COMO O**RGANIZACIONALES**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTE DOCUMENTO

4.3 DISEÑO DE CONTROLES

EL DISEÑO DE **CADA CONTROL CONTIENE LO SIGUIENTE**:

- **TÍTULO DE CONTROL**: NOMBRE CORTO DEL CONTROL
- **TABLA DE ATRIBUTOS**: UNA TABLA MUESTRA EL VALOR DE CADA ATRIBUTO PARA EL CONTROL DADO
- **CONTROL**: CUÁL ES EL CONTROL
- **PROPÓSITO**: POR QUÉ SE DEBE IMPLEMENTAR EL CONTROL
- **GUÍA**: CÓMO SE DEBE IMPLEMENTAR EL CONTROL
- **OTRA INFORMACIÓN**: TEXTO EXPLICATIVO O REFERENCIAS A OTROS DOCUMENTOS RELACIONADOS

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. EJEMPLO DE CONTROL

TÍTULO DE CONTROL

5.3 SEGREGACIÓN DE FUNCIONES

TABLA DE ATRIBUTOS

Tipo de control	Información propiedades de seguridad	La seguridad cibernética conceptos	Operacional capacidades	Dominios de seguridad
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	# Gobernanza #identidad_y_ac-cess_management	# Gobernanza_y_Ecosistema

CONTROL

DEBEN SEGREGARSE LOS DEBERES CONFLICTIVOS Y LAS ÁREAS CONFLICTIVAS DE RESPONSABILIDAD

PROPÓSITO

REDUCIR EL RIESGO DE FRAUDE, ERROR Y ELUSIÓN DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. EJEMPLO DE CONTROL

GUÍA

LA SEGREGACIÓN DE DEBERES Y ÁREAS DE RESPONSABILIDAD TIENE COMO OBJETIVO SEPARAR LOS DEBERES EN CONFLICTO ENTRE DIFERENTES INDIVIDUOS PARA EVITAR QUE UN INDIVIDUO EJECUTE DEBERES POTENCIALMENTE CONFLICTIVOS POR SU CUENTA.

LA ORGANIZACIÓN DEBE DETERMINAR QUÉ DEBERES Y ÁREAS DE RESPONSABILIDAD DEBEN SEGREGARSE. LOS SIGUIENTES SON EJEMPLOS DE ACTIVIDADES QUE PUEDEN REQUERIR SEGREGACIÓN:

a) INICIAR, APROBAR Y EJECUTAR UN CAMBIO;
b) SOLICITAR, APROBAR E IMPLEMENTAR DERECHOS DE ACCESO;
c) DISEÑAR, IMPLEMENTAR Y REVISAR EL CÓDIGO;
d) DESARROLLAR SOFTWARE Y ADMINISTRAR SISTEMAS DE PRODUCCIÓN;
e) USAR Y ADMINISTRAR APLICACIONES;
f) USO DE APLICACIONES Y BASES DE DATOS DE ADMINISTRACIÓN;
g) DISEÑAR, AUDITAR Y ASEGURAR LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. EJEMPLO DE CONTROL

GUÍA

SE DEBE CONSIDERAR LA POSIBILIDAD DE COLUSIÓN AL DISEÑAR LOS CONTROLES DE SEGREGACIÓN. LAS ORGANIZACIONES PEQUEÑAS PUEDEN ENCONTRAR DIFÍCIL LOGRAR LA SEGREGACIÓN DE FUNCIONES, PERO EL PRINCIPIO DEBE APLICARSE EN LA MEDIDA DE LO POSIBLE Y PRACTICABLE. SIEMPRE QUE SEA DIFÍCIL SEGREGAR, SE DEBEN CONSIDERAR OTROS CONTROLES, COMO EL SEGUIMIENTO DE LAS ACTIVIDADES, LAS PISTAS DE AUDITORÍA Y LA SUPERVISIÓN DE LA GESTIÓN.

SE DEBE TENER CUIDADO UTILIZAR SISTEMAS DE CONTROL DE ACCESO BASADOS EN ROLES PARA GARANTIZAR QUE A LAS PERSONAS NO SE LES OTORGUEN ROLES EN CONFLICTO. CUANDO HAY UNA GRAN CANTIDAD DE ROLES, LA ORGANIZACIÓN DEBE CONSIDERAR EL USO DE HERRAMIENTAS AUTOMATIZADAS PARA IDENTIFICAR CONFLICTOS Y FACILITAR SU ELIMINACIÓN. LOS ROLES DEBEN DEFINIRSE Y APROVISIONARSE CUIDADOSAMENTE PARA MINIMIZAR LOS PROBLEMAS DE ACCESO SI SE ELIMINA O REASIGNA UN ROL.

GUÍA

NINGUNA OTRA INFORMACIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTA NORMA

CAPÍTULOS DE CONTROLES DE SEGURIDAD

- **5. CONTROLES ORGANIZACIONALES**
- **6. CONTROLES DE PERSONAS**
- **7. CONTROLES FÍSICOS**
- **8. CONTROLES TECNOLÓGICOS**

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

6.1 Selección
6.2 Términos y condiciones de empleo
6.3 Conciencia de seguridad, educación y capacitación de la información
6.4 Proceso Disciplinario
6.5 Responsabilidades después de la terminación o cambio de empleo
6.6 Acuerdos de confidencialidad o no divulgación
6.7 Trabajo remoto
6.8 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

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

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.1	**Políticas para la seguridad de la información**	05.1.1, 05.1.2	La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.
5.2	**Roles y responsabilidades de seguridad de la información**	06.1.1	Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
5.3	**Segregación de tareas**	06.1.2	Deben segregarse los deberes conflictivos y las áreas conflictivas de responsabilidad.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.4	**Responsabilidades de la dirección**	07.2.1	La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.
5.5	**Contacto con las autoridades**	06.1.3	La organización debe establecer y mantener contacto con las autoridades pertinentes.
5.6	**Contacto con grupos de interés especial**	06.1.4	La organización debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
5.7	**Inteligencia de amenazas**	**Nuevo Control**	La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para generar información sobre amenazas.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.8	**Seguridad de la información en la gestión de proyectos**	06.1.5. 14.1.1	La seguridad de la información debe integrarse en la gestión de proyectos.
5.9	**Inventario de información y otros activos asociados**	08.1.1, 08.1.2	Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.
5.10	**Uso aceptable de información y otros activos asociados**	08.1.3, 08.2.3	Deben identificarse, documentarse e implementarse reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.
5.11	**Devolución de activos**	08.1.4	El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.12	**Clasificación de información**	08.2.1	La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.
5.13	**Etiquetado de información**	08.2.2	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.14	**Transferencia de información**	13.2.1, 13.2.2, 13.2.3	Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
5.15	**Control de acceso**	09.1.1, 09.1.2	Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos comerciales y de seguridad de la información.
5.16	**Gestión de identidad**	09.2.1	Debe gestionarse el ciclo de vida completo de las identidades.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.17	**Información de autenticación**	09.2.4, 09.3.1, 09.4.3	La asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.
5.18	**Derechos de acceso**	09.2.2, 09.2.5. 09.2.6	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.
5.19	**Seguridad de la información en las relaciones con los proveedores**	15.1.1	Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.20	**Abordar la seguridad de la información dentro de los acuerdos de proveedores**	15.1.2	Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor.
5.21	**Gestión de la seguridad de la información en la cadena de suministro de las TIC**	15.1.3	Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.
5.22	**Seguimiento, revisión y gestión de cambios de servicios de proveedores**	15.2.1, 15.2.2	La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.23	**Seguridad de la información para el uso de servicios en la nube**	Nuevo Control	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.
5.24	**Planificación y preparación de la gestión de incidentes de seguridad de la información**	16.1.1	La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información.
5.25	**Evaluación y decisión sobre eventos de seguridad de la información**	16.1.4	La organización debería evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.26	**Respuesta a incidentes de seguridad de la información**	16.1.5	Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.
5.27	**Aprender de los incidentes de seguridad de la información**	16.1.6	El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.
5.28	**Recopilación de evidencia**	16.1.7	La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.29	**Seguridad de la información durante la interrupción**	17.1.1, 17.1.2, 17.1.3	La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.
5.30	**Preparación para las TIC para la continuidad del negocio**	Nuevo Control	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
5.31	**Identificación de requisitos legales, reglamentarios y contractuales**	18.1.1, 18.1.5	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.32	**Derechos de propiedad intelectual (DPI)**	18.1.2	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
5.33	**Protección de los registros**	18.1.3	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.
5.34	**Privacidad y protección de datos de carácter personal (DCP)**	18.1.4	La organización debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 5 CONTROLES ORGANIZACIONALES

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
5.35	**Revisión independiente de la seguridad de la información**	18.2.1	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, debe revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
5.36	**Cumplimiento de las políticas y normas de seguridad de la información**	18.2.2, 18.2.3	El cumplimiento de la política de seguridad de la información de la organización, las políticas específicas del tema, las reglas y los estándares debe revisarse periódicamente.
5.37	**Documentación de procedimientos operacionales**	12.1.1	Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 6 CONTROLES DE PERSONAS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
6.1	**Comprobación**	07.1.1	Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y los riesgos percibidos.
6.2	**Términos y condiciones de contratación**	07.1.2	Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 6 CONTROLES DE PERSONAS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
6.3	**Concienciación, educación y formación en seguridad de la información**	07.2.2	El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas sobre la seguridad de la información y actualizaciones regulares de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.
6.4	**Proceso disciplinario**	07.2.3	Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 6 CONTROLES DE PERSONAS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
6.5	**Responsabilidades ante la finalización o cambio**	07.3.1	Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o el cambio de empleo deben definirse, aplicarse y comunicarse al personal pertinente y otras partes interesadas.
6.6	**Acuerdos de confidencialidad o no divulgación**	13.2.4	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 6 CONTROLES DE PERSONAS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
6.7	**Teletrabajo**	06.2.2	Se deben implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.
6.8	**Notificación de los eventos de seguridad de la información**	16.1.2, 16.1.3	La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 7 CONTROLES FÍSICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
7.1	**Perímetro de seguridad física**	11.1.1	Los perímetros de seguridad deben definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.
7.2	**Controles físicos de entrada**	11.1.2, 11.1.6	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.
7.3	**Seguridad de oficinas, despachos y recursos**	11.1.3	Debe diseñarse e implementarse la seguridad física de las oficinas, salas e instalaciones.
7.4	**Monitorización de la seguridad física**	**Nuevo Control**	Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 7 CONTROLES FÍSICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
7.5	**Protección contra las amenazas externas y ambientales**	11.1.4	Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.
7.6	**El trabajo en áreas seguras**	11.1.5	Se deben diseñar e implementar medidas de seguridad para trabajar en áreas seguras.
7.7	**Puesto de trabajo despejado y pantalla limpia**	11.2.9	Deben definirse y aplicarse adecuadamente reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y reglas de pantalla limpia para las instalaciones de procesamiento de información.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 7 CONTROLES FÍSICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
7.8	**Emplazamiento y protección de equipos**	11.2.1	El equipo debe estar ubicado de forma segura y protegida.
7.9	**Seguridad de los equipos fuera de las instalaciones**	11.2.6	Los activos fuera del sitio deben estar protegidos.
7.10	**Soportes de almacenamiento**	08.3.1, 08.3.2, 08.3.3, 11.2.5	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
7.11	**Instalaciones de suministro**	11.2.2	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 7 CONTROLES FÍSICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
7.12	**Seguridad del cableado**	11.2.3	Los cables que transportan energía, datos o servicios de información de apoyo deben protegerse contra intercepciones, interferencias o daños.
7.13	**Mantenimiento de los equipos**	11.2.4	El equipo debe mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.
7.14	**Eliminación o reutilización segura de los equipos**	11.2.7	Los elementos del equipo que contengan medios de almacenamiento deben verificarse para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.1	**Dispositivos finales de usuario**	06.2.1, 11.2.8	La información almacenada, procesada o accesible a través de los dispositivos finales de los usuarios debe protegerse.
8.2	**Gestión de privilegios de acceso**	09.2.3	La asignación y el uso de derechos de acceso privilegiado deben restringirse y gestionarse.
8.3	**Restricción del acceso a la información**	09.4.1	El acceso a la información y otros activos asociados debe estar restringido de acuerdo con la política específica del tema establecida sobre control de acceso.
8.4	**Acceso al código fuente**	09.4.5	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software debe administrarse adecuadamente.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.5	**Autenticación segura**	09.4.2	Las tecnologías y los procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
8.6	**Gestión de capacidades**	12.1.3	El uso de los recursos debe monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.
8.7	**Controles contra el código malicioso**	12.2.1	La protección contra el malware debe implementarse y respaldarse mediante la conciencia adecuada del usuario.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.8	**Gestión de vulnerabilidades técnicas**	12.6.1, 18.2.3	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
8.9	**Gestión de la configuración**	**Nuevo Control**	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
8.10	**Eliminación de la información**	**Nuevo Control**	La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.11	**Enmascaramiento de datos**	Nuevo Control	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
8.12	**Prevención de fugas de datos**	Nuevo Control	Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.13	**Copias de seguridad de la información**	12.3.1	Las copias de respaldo de la información, el software y los sistemas deben mantenerse y probarse regularmente de acuerdo con la política de respaldo específica del tema acordada.
8.14	**Redundancia de los recursos de tratamiento de la información**	17.2.1	Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.
8.15	**Registros de eventos**	12.4.1, 12.4.2, 12.4.3	Se deben producir, almacenar, proteger y analizar registros que registren actividades, excepciones, fallas y otros eventos relevantes.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.16	**Seguimiento de actividades**	**Nuevo Control**	Las redes, los sistemas y las aplicaciones deben monitorearse para detectar comportamientos anómalos y deben tomarse las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.
8.17	**Sincronización del reloj**	12.4.4	Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con las fuentes de tiempo aprobadas.
8.18	**Uso de los programas de utilidad con privilegios**	09.4.4	El uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones debe restringirse y controlarse estrictamente.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.19	**Instalación de software en sistemas operativos**	12.5.1, 12.6.2	Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.
8.20	**Seguridad de redes**	13.1.1	Las redes y los dispositivos de red deben protegerse, administrarse y controlarse para proteger la información en los sistemas y aplicaciones.
8.21	**Seguridad de los servicios de red**	13.1.2	Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red deben identificarse, implementarse y monitorearse.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.22	**Segregación en redes**	13.1.3	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.
8.23	**Filtrado de webs**	**Nuevo Control**	El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.
8.24	**Uso de la criptografía**	10.1.1, 10.1.2	Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.
8.25	**Seguridad en el ciclo de vida del desarrollo**	14.2.1	Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.26	**Requisitos de seguridad de las aplicaciones**	14.1.2, 14.1.3	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.
8.27	**Arquitectura segura de sistemas y principios de ingeniería**	14.2.5	Los principios para diseñar sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.
8.28	**Codificación segura**	Nuevo Control	Los principios de codificación segura deben aplicarse al desarrollo de software.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.29	**Pruebas de seguridad en desarrollo y aceptación**	14.2.8. 14.2.9	Los procesos de prueba de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.
8.30	**Externalización del desarrollo**	14.2.7	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
8.31	**Separación de entornos de desarrollo, prueba y producción**	12.1.4, 14.2.6	Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002. 8 CONTROLES TECNOLÓGICOS

27002 2022	CONTROL	27002 2013	DESCRIPCIÓN 27002:2022
8.32	**Gestión de cambios**	12.1.2, 14.2.2, 14.2.3, 14.2.4	Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
8.33	**Datos de prueba**	14.3.1	La información de las pruebas debe seleccionarse, protegerse y gestionarse adecuadamente.
8.34	**Protección de sistemas de información durante las pruebas de auditoría**	12.7.1	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

ESTE ANEXO PROPORCIONA UNA TABLA PARA DEMOSTRAR EL USO DE ATRIBUTOS COMO UNA FORMA DE CREAR DIFERENTES VISTAS DE LOS CONTROLES. LOS CINCO EJEMPLOS DE ATRIBUTOS SON:

A. TIPOS DE CONTROL

#PREVENTIVO, #DETECTIVO, #CORRECTIVO

B. PROPIEDADES DE SEGURIDAD DE LA INFORMACIÓN

#CONFIDENCIALIDAD, #INTEGRIDAD, #DISPONIBILIDAD

C. CONCEPTOS DE CIBERSEGURIDAD

#IDENTIFICAR, #PROTEGER, #DETECTAR, #RESPONDER, #RECUPERAR

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

D. CAPACIDADES OPERATIVAS

#GOBERNANZA, #GESTIÓN_DE_ACTIVOS, #PROTECCIÓN_DE_LA_INFORMACIÓN, #SEGURIDAD_DE_RECURSOS_HUMANOS, #SEGURIDAD_FÍSICA, #SEGURIDAD_DE_SISTEMAS_Y_REDES, #SEGURIDAD_DE_APLICACIONES, #CONFIGURACIÓN_SEGURA, # GESTIÓN_DE_IDENTIDAD_Y_ACCESO, #GESTIÓN_DE_AMENAZAS_Y_VULNERABILIDADES, #CONTINUIDAD, #SEGURIDAD_DE_RELACIONES_CON_PROVEEDORES, #CUMPLIMIENTO_Y_LEGAL, #GESTIÓN_DE_EVENTOS_DE_SEGURIDAD_DE_LA_INFORMACIÓN, #GARANTÍA_DE_SEGURIDAD_DE_LA_INFORMACIÓN

E. DOMINIOS DE SEGURIDAD

#GOBERNANZA_Y_ECOSISTEMA, #PROTECCIÓN, #DEFENSA, #RESILIENCIA

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
5.1	Políticas para información seguridad	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernanza_ y_Ecosys- artículo # Resil- iencia
5.2	Información roles de seguridad y responsabilidad Habilidades	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernar- ance_y_ Ecosistema # Proteccion # Resiliencia
5.3	segregación de deberes	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Gobernanza # Identidad_y_ access_man- gestion	# Gobernanza_ y_Ecosys- tiempo
5.4	Gestión responsable corbatas	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Gobernanza	# Gobernanza_ y_Ecosys- tiempo
5.5	Contactar con autoridades	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar #Responder # recuperar	# Gobernanza	# Defensa # Re- silencio

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
5.11	Retorno de activos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Asset_man-gestion	# Proteccion
5.12	Clasificación de información	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Información_ proteccion	# Proteccion # Defensa
5.13	Etiquetado de información	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Información_ proteccion	# Defensa # Proteccion
5.14	Información transferir	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Asset_man-gestion # Información_ proteccion	# Proteccion
5.15	Control de acceso	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man-gestion	# Proteccion
5.16	hombre de identidad-gestion	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man-gestion	# Proteccion

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
5.17	Autenticación información	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man- gestion	# Proteccion
5.18	Derechos de acceso	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man- gestion	# Proteccion
5.19	Información seguridad en relación con el proveedor naciones	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción
5.20	Direccionamiento información seguridad con- en proveedor acuerdos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción
5.21	Gerente información seguridad en la oferta TIC cadena	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	# Proveedor_re- lationships_se- seguridad	# Gobernanza_ y_Ecosys- artículo # ción

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
5.22	Monitor-ing, revisión y cambio administración de proveedor servicios	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# identificar	# Proveedor_re-lationships_se-seguridad	# Gobernanza_y_Ecosys-artículo # ción #Defensa # Información_seguridad_como-seguro
5.23	Información seguridad para uso de la nube servicios	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Proveedor_re-lationships_se-seguridad	# Gobernanza_y_Ecosys-artículo # ción
5.24	Información incidente de seguridad manejo de abolladuras - planeación mental y prepara-ción	# Correctivo	# Confidencial-#Integridad # Disponibilidad	# Responder # Re-cubrir	# Gobernanza # Informa-tion_securi-ty_event_man-gestion	# Defensa

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
5.25	Evaluación y decisión sobre información ción de seguridad eventos	# Detective	# Confidencial- #Integridad # Disponibilidad	# Detectar # Re- responder	# Informa- tion_securi- ty_event_man- gestion	# Defensa
5.26	Respuesta a información incidente de seguridad abolladuras	# Correctivo	# Confidencial- #Integridad # Disponibilidad	# Responder # Re- cubrir	# Informa- tion_securi- ty_event_man- gestion	# Defensa
5.27	Aprendiendo de información incidente de seguridad abolladuras	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	# Informa- tion_securi- ty_event_man- gestion	# Defensa
5.28	Colección de evidencia	# Correctivo	# Confidencial- #Integridad # Disponibilidad	# Detectar # Re- responder	# Informa- tion_securi- ty_event_man- gestion	# Defensa

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
5.29	Información seguridad durante- en interrupción	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Re- responder	# Continuidad	# Proteccion # Resiliencia
5.30	preparación para las TIC para negocios continuidad	# Correctivo	# Disponibilidad	# Responder	# Continuidad	# Resiliencia
5.31	legal, estatutario ry, regulador y contrato- requerimiento tual mentos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	#Legal_y_ cumplimiento	# Gobernanza_ y_Ecosys- artículo # ción
5.32	Intelectual propiedad derechos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# identificar	#Legal_y_ cumplimiento	# Gobernanza_ y_Ecosys- tiempo
5.33	Proteccion DE registros	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	#Legal_y_ cumplimiento # Asset_man- gestion # Información_ proteccion	# Defensa

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
5.34	Privacidad y proteccion DE información personal	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	# Información_ proteccion #Legal_y_ cumplimiento	# Proteccion
5.35	Independiente repaso de información seguridad	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	# Información_ seguridad_como- seguro	# Gobernanza_ y_Ecosys- tiempo
5.36	Cumplimiento con políticas, reglas y normas para información seguridad	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Identificar # Pro- tectar	#Legal_y_ cumplimiento # Información_ seguridad_como- seguro	# Gobernanza_ y_Ecosys- tiempo

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
5.37	documentado operando procedimientos	# Preventivo # Correctivo	# Confidencial- #Integridad # Disponibilidad	# Proteger # Re- cubrir	# Asset_man- gestion # fisio- cal_seguridad # Sistema_y_ network_secu- ridad # Aplica- ción_seguridad # Secure_con- figuración # Identidad_ y_acceso_ administración # amenaza_y_ vulnerabilidad_ administración # Continuidad # Informa- tion_securi- ty_event_man- gestion	# Gobernanza_ y_Ecosys- artículo # ción #Defensa

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
6.1	Poner en pantalla	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Human_re-source_secu-ridad	# Gobernanza_y_Ecosys-tiempo
6.2	Términos y condiciones de empleo	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Human_re-source_secu-ridad	# Gobernanza_y_Ecosys-tiempo
6.3	Información seguridad conciencia, educación y capacitación	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Human_re-source_secu-ridad	# Gobernanza_y_Ecosys-tiempo
6.4	Disciplinario proceso	# Preventivo # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Proteger # Re-responder	# Human_re-source_secu-ridad	# Gobernanza_y_Ecosys-tiempo

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
6.5	responsabilidad Habilidades después terminación o cambio de empleo	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Human_resource_seguridad #Activo_administración	# Gobernanza_y_Ecosys-tiempo
6.6	confiado-lidad o no divulgación acuerdos	# Preventivo	# Confidencial alidad	# Proteger	# Human_resource_security #Information_protección # Proveedor_relaciones	# Gobernanza_y_Ecosys-tiempo
6.7	Trabajo remoto-En g	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Asset_mangestion # Información_proteccion # Physical_seseguridad # System_and_net-trabajo_seguridad	# Proteccion

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
6.8	Información evento de seguridad reportando	# Detective	# Confidencial- #Integridad # Disponibilidad	# Detectar	# Informa- tion_securi- ty_event_man- gestion	# Defensa
7.1	Seguridad física perimetral- tercera	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_se- seguridad	# Proteccion
7.2	Entrada física	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_se- seguridad # Iden- tity_and_Ac- cess_Manage- mento	# Proteccion
7.3	Oficina de seguridad es, habitaciones y instalaciones	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_se- calidad #Activo_ administración	# Proteccion
7.4	Seguridad física monitor de rity- En g	# Preventivo # Detective	# Confidencial- #Integridad # Disponibilidad	# Proteger # De- tectar	# Physical_se- seguridad	# Proteccion # Defensa

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
7.5	Proteger- en contra físico y ambiental amenazas	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_se- seguridad	# Proteccion
7.6	Trabajando en áreas seguras	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_se- seguridad	# Proteccion
7.7	Limpiar el escritorio y pantalla clara	# Preventivo	# Confidencial alidad	# Proteger	# Physical_se- seguridad	# Proteccion
7.8	Equipo ubicación y proteccion	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_se- calidad #Activo_ administración	# Proteccion
7.9	seguridad de as- pone en marcha ises	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_se- calidad #Activo_ administración	# Proteccion
7.10	Medios de almacenamiento	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Physical_se- calidad #Activo_ administración	# Proteccion

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
7.11	Secundario utilidades	# Preventivo # Detective	# Integridad # Disponibilidad	# Proteger # De-tectar	# Physical_se-seguridad	# Proteccion
7.12	Cableado seguro ridad	# Preventivo	# Confidencial alidad # disponible-habilidad	# Proteger	# Physical_se-seguridad	# Proteccion
7.13	Equipo mantenimiento	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Physical_se-calidad #Activo_ administración	# Proteccion # Resiliencia
7.14	Eliminación segura al o reutilización de equipo	# Preventivo	# Confidencial alidad	# Proteger	# Physical_se-calidad #Activo_ administración	# Proteccion
8.1	Punto final de usuario dispositivos	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Asset_man-gestion # Información_ proteccion	# Proteccion
8.2	Privilegiado derechos de acceso	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man-gestion	# Proteccion

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.3	Información Restricción de acceso- ción	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man- gestion	# Proteccion
8.4	El acceso a los código fuente	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_ y_acceso_ administración # Aplica- ción_seguridad # Secure_con- figuración	# Proteccion
8.5	autenticación segura ticación	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Identidad_y_ access_man- gestion	# Proteccion
8.6	capacidad hombre- gestion	# Preventivo # Detective	# Integridad # Disponibilidad	# Identificar # Pro- detectar #Detectar	# Continuidad	# Gobernanza_ y_Ecosys- artículo # ción

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.7	Proteccion contra mal-Cierto	# Preventivo # Detective # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Proteger # De-tectar	# Sistema_y_ network_secu-ridad # Informa-tion_protec-ción	# Proteccion # Defensa
8.8	Gestión de técnico vulnerabilidades	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Identificar # Pro-tectar	# amenaza_y_ vulnerabilidad_ administración	# Gobernanza_ y_Ecosys-artículo # ción #Defensa
8.9	Configuración administración	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Secure_con-figuración	# Proteccion
8.10	Información supresión	# Preventivo	# Confidencial alidad	# Proteger	# Información_ proteccion #Legal_y_ cumplimiento	# Proteccion
8.11	Enmascaramiento de datos	# Preventivo	# Confidencial alidad	# Proteger	# Información_ proteccion	# Proteccion

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.12	Fuga de datos prevención	# Preventivo # Detective	# Confidencial alidad	# Proteger # De-tectar	# Información_ proteccion	# Proteccion # Defensa
8.13	Información respaldo	# Correctivo	# Integridad # Disponibilidad	# recuperar	# Continuidad	# Proteccion
8.14	Redundancia de información Procesando instalaciones	# Preventivo	# Disponibilidad	# Proteger	# Continuidad # Asset_man-gestion	# Proteccion # Resiliencia
8.15	Inicio sesión	# Detective	# Confidencial-#Integridad # Disponibilidad	# Detectar	# Informa-tion_securi-ty_event_man-gestion	# Proteccion # Defensa
8.16	Supervisión ocupaciones	# Detective # Correctivo	# Confidencial-#Integridad # Disponibilidad	# Detectar # Re-responder	# Informa-tion_securi-ty_event_man-gestion	# Defensa

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.17	Reloj síncronización	# Detective	# Integridad	# Proteger # Detectar	# Information_security_event_mangestion	# Proteccion # Defensa
8.18	uso de utilidad legítima programas	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Sistema_y_network_security #Secure_configuración # Solicitud_seguridad	# Proteccion
8.19	Instalación de software en Operacional sistemas	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Secure_configuración # Solicitud_seguridad	# Proteccion

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.20	Redes seguridad	# Preventivo # Detective	# Confidencial- #Integridad # Disponibilidad	# Proteger # De- tectar	# Sistema_y_ network_secu- ridad	# Proteccion
8.21	Seguridad de servicio de red vicios	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Sistema_y_ network_secu- ridad	# Proteccion
8.22	segregación de redes	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Sistema_y_ network_secu- ridad	# Proteccion
8.23	Filtrado web	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Sistema_y_ network_secu- ridad	# Proteccion
8.24	Uso de crip- tografia	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Secure_con- figuración	# Proteccion

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.25	desarrollo seguro opment vida ciclo	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Aplica- ción_seguridad # Sistema_y_ network_secu- ridad	# Proteccion
8.26	Solicitud re-seguridad requisitos	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Aplica- ción_seguridad # Sistema_y_ network_secu- ridad	# Proteccion # Defensa
8.27	sistema seguro arquitectura e ingeniero- principios de formación	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Aplica- ción_seguridad # Sistema_y_ network_secu- ridad	# Proteccion
8.28	Codificación segura	# Preventivo	# Confidencial- #Integridad # Disponibilidad	# Proteger	# Aplica- ción_seguridad # Sistema_y_ network_secu- ridad	# Proteccion

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.29	Seguridad prueba en de-desarrollo y aceptación	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# identificar	# Aplica-ción_seguridad # Informa-tion_securi-ty_assurance # Sistema_y_ network_secu-ridad	# Proteccion
8.30	subcontratado desarrollo	# Preventivo # Detective	# Confidencial-#Integridad # Disponibilidad	# Identificar # Pro-detectar #Detectar	# Sistema_y_ network_secu-ridad # Aplica-ción_seguridad # Proveedor_re-lationships_se-seguridad	# Gobernanza_ y_Ecosys-artículo # ción

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO A (INFORMATIVO) ATRIBUTOS DE USO

YO ASI / CEI 27002 control identificar	nombre de control	Tipo de control	Información seguridad propiedades	La seguridad cibernética conceptos	Operacional capacidades	Seguridad dominios
8.31	Separación de desarrollo-prueba, prueba y producción ambientes	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Aplica-ción_seguridad # Sistema_y_network_secu-ridad	# Proteccion
8.32	Cambia hombre - gestion	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Aplica-ción_seguridad # Sistema_y_network_secu-ridad	# Proteccion
8.33	Prueba de información ción	# Preventivo	# Confidencial-#Integridad	# Proteger	# Información_proteccion	# Proteccion
8.34	Proteccion de información sistemas de ción durante la auditoría pruebas	# Preventivo	# Confidencial-#Integridad # Disponibilidad	# Proteger	# Sistema_y_network_secu-ridad # Informa-tion_protec-ción	# Gobernanza_y_Ecosys-artículo # ción

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022 (ESTE DOCUMENTO) CON ISO/IEC 27002:2013

EL PROPÓSITO DE ESTE ANEXO ES PROPORCIONAR COMPATIBILIDAD CON VERSIONES ANTERIORES DE ISO/IEC 27002:2013 PARA LAS ORGANIZACIONES QUE ACTUALMENTE USAN ESE ESTÁNDAR Y AHORA DESEAN HACER LA TRANSICIÓN A ESTA EDICIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
5.1	05.1.1, 05.1.2	Políticas de seguridad de la información
5.2	06.1.1	Roles y responsabilidades de seguridad de la información
5.3	06.1.2	Segregación de deberes
5.4	07.2.1	responsabilidades de gestión
5.5	06.1.3	Contacto con autoridades
5.6	06.1.4	Contacto con grupos de interés especial
5.7	Nuevo	Inteligencia de amenazas
5.8	06.1.5, 14.1.1	Seguridad de la información en la gestión de proyectos.
5.9	08.1.1, 08.1.2	Inventario de información y otros activos asociados
5.10	08.1.3, 08.2.3	Uso aceptable de la información y otros activos asociados

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
5.11	08.1.4	Devolución de activos
5.12	08.2.1	Clasificación de la información
5.13	08.2.2	Etiquetado de información
5.14	13.2.1, 13.2.2, 13.2.3	Transferencia de información
5.15	09.1.1, 09.1.2	Control de acceso
5.16	09.2.1	Gestión de identidad
5.17	09.2.4, 09.3.1, 09.4.3	Información de autenticación

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
5.18	09.2.2, 09.2.5, 09.2.6	Derechos de acceso
5.19	15.1.1	Seguridad de la información en las relaciones con los proveedores
5.20	15.1.2	Abordar la seguridad de la información en los acuerdos con los proveedores
5.21	15.1.3	Gestión de la seguridad de la información en la cadena de suministro de las TIC
5.22	15.2.1, 15.2.2	Seguimiento, revisión y gestión de cambios de servicios de proveedores
5.23	Nuevo	Seguridad de la información para el uso de servicios en la nube
5.24	16.1.1	Planificación y preparación de la gestión de incidentes de seguridad de la información
5.25	16.1.4	Evaluación y decisión sobre eventos de seguridad de la información

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
5.26	16.1.5	Respuesta a incidentes de seguridad de la información
5.27	16.1.6	Aprender de los incidentes de seguridad de la información
5.28	16.1.7	Recolección de evidencia
5.29	17.1.1, 17.1.2, 17.1.3	Seguridad de la información durante la interrupción
5.30	Nuevo	Preparación de las TIC para la continuidad del negocio
5.31	18.1.1, 18.1.5	Requisitos legales, estatutarios, reglamentarios y contractuales
5.32	18.1.2	Derechos de propiedad intelectual
5.33	18.1.3	Protección de registros
5.34	18.1.4	Privacidad y protección de PII
5.35	18.2.1	Revisión independiente de la seguridad de la información.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
5.36	18.2.2, 18.2.3	Cumplimiento de políticas, normas y estándares de seguridad de la información
5.37	12.1.1	Procedimientos operativos documentados
6.1	07.1.1	Poner en pantalla
6.2	07.1.2	Términos y condiciones de empleo
6.3	07.2.2	Concientización, educación y capacitación en seguridad de la información
6.4	07.2.3	Proceso Disciplinario
6.5	07.3.1	Responsabilidades después de la terminación o cambio de empleo
6.6	13.2.4	Acuerdos de confidencialidad o no divulgación
6.7	06.2.2	Trabajo remoto

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
6.8	16.1.2, 16.1.3	Informes de eventos de seguridad de la información
7.1	11.1.1	Perímetros físicos de seguridad
7.2	11.1.2, 11.1.6	Entrada física
7.3	11.1.3	Asegurar oficinas, salas e instalaciones
7.4	Nuevo	Monitoreo de seguridad física
7.5	11.1.4	Protección contra amenazas físicas y ambientales.
7.6	11.1.5	Trabajar en áreas seguras
7.7	11.2.9	Escritorio despejado y pantalla despejada
7.8	11.2.1	Emplazamiento y protección de equipos

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
7.9	11.2.6	Seguridad de los activos fuera de las instalaciones
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Medios de almacenamiento
7.11	11.2.2	Utilidades de apoyo
7.12	11.2.3	seguridad del cableado
7.13	11.2.4	Mantenimiento de equipo
7.14	11.2.7	Eliminación segura o reutilización de equipos
8.1	06.2.1, 11.2.8	Dispositivos de punto final de usuario
8.2	09.2.3	Derechos de acceso privilegiado
8.3	09.4.1	Restricción de acceso a la información

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
8.4	09.4.5	Acceso al código fuente
8.5	09.4.2	Autenticación segura
8.6	12.1.3	Gestión de capacidad
8.7	12.2.1	Protección contra malware
8.8	12.6.1, 18.2.3	Gestión de vulnerabilidades técnicas
8.9	Nuevo	Gestión de la configuración
8.10	Nuevo	Eliminación de información
8.11	Nuevo	Enmascaramiento de datos

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
8.12	Nuevo	Prevención de fuga de datos
8.13	12.3.1	Copia de seguridad de la información
8.14	17.2.1	Redundancia de las instalaciones de procesamiento de información
8.15	12.4.1, 12.4.2, 12.4.3	Inicio sesión
8.16	Nuevo	Actividades de seguimiento
8.17	12.4.4	Sincronización de reloj
8.18	09.4.4	Uso de programas de utilidad privilegiados
8.19	12.5.1, 12.6.2	Instalación de software en sistemas operativos
8.20	13.1.1	Seguridad en redes

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
8.21	13.1.2	Seguridad de los servicios de red.
8.22	13.1.3	Segregación de redes
8.23	Nuevo	Filtrado web
8.24	10.1.1, 10.1.2	Uso de criptografía
8.25	14.2.1	Ciclo de vida de desarrollo seguro
8.26	14.1.2, 14.1.3	Requisitos de seguridad de la aplicación
8.27	14.2.5	Principios de arquitectura e ingeniería de sistemas seguros
8.28	Nuevo	Codificación segura

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ANEXO B (INFORMATIVO) CORRESPONDENCIA DE ISO/IEC 27002:2022

Tabla B.1 - Correspondencia entre controles en este documento y controles en ISO/IEC 27002: 2013

YO ASI / CEI 27002: 2022 control identificar	ISO / CEI 27002: 2013 identificador de control	nombre de control
8.29	14.2.8, 14.2.9	Pruebas de seguridad en desarrollo y aceptación.
8.30	14.2.7	Desarrollo subcontratado
8.31	12.1.4, 14.2.6	Separación de los entornos de desarrollo, prueba y producción
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Gestión del cambio
8.33	14.3.1	Información de prueba
8.34	12.7.1	Protección de los sistemas de información durante las pruebas de auditoría

ESTO ES TODO