ISO 27001:2022

Sistemas de Gestión de Seguridad de la Información

Área de Seguridad de la Información

Nuestra estrategia,
el DESARROLLO COMPETITIVO.

Intedya®
International Dynamic Advisors

INTEDYA, la mayor firma internacional especializada en la **consultoría, auditoría y formación** en materia de gestión de riesgos y cumplimiento normativo bajo estándares internacionalmente reconocidos en materia de Calidad, Sostenibilidad, Gestión de Riesgos y Cumplimiento y Salud e Inocuidad Alimentaria, en organizaciones públicas y privadas de cualquier tipo de actividad y dimensión.

"Apostando por **el DESARROLLO COMPETITIVO.**"

Certificación DE PERSONAS

Presencia DIRECTA en 17 PAISES

España
Portugal
México
Brasil
Colombia
Ecuador
Perú
Argentina
Rep. Dominicana
Chile
Honduras
Guatemala
Costa Rica
Panamá
Paraguay
Uruguay
Bolivia

+ 80 OFICINAS INTEDYA

EQUIPO INTERNACIONAL DE +500 PERSONAS

MÁS DE 20000 EMPRESAS CLIENTE

17867	38390	347	37	25	132
PROYECTOS DE CONSULTORÍA EJECUTADOS	**ALUMNOS FORMADOS** EN CAMPUS E-LEARNING	**CURSOS E-LEARNING** DISPONIBLES	**TITULACIONES** COMO AUDITOR	**TITULACIONES UNI-VERSITARIAS**	**MÁSTERCLASS** ANUALES

ALIANZAS, MEMBRESÍAS Y LIDERAZGO

La **NORMA ISO 27001:2022** establece los requisitos para una gestión eficaz de los riesgos que pueden afectar a la confidencialidad, la integridad y la disponibilidad de la información.

Esta norma tiene **vocación universal**, es aplicable a **ORGANIZACIONES DE TODOS LOS SECTORES Y TAMAÑOS**, y describe de qué debe constar un sistema de gestión de la seguridad de la información en cualquier tipo de organización.

La norma es especialmente útil cuando la **PROTECCIÓN DE LA INFORMACIÓN ES CRÍTICA**, por ejemplo, en las áreas de gobierno, banca y finanzas, legal, salud, empresas de servicios de tecnología de la información o comunicaciones, o cualquier otro ámbito donde los **activos de información** requieran de una adecuada protección.

EVOLUCIÓN

ISO/IEC 27002:2022

ISO/IEC 27001:2022

Los datos son claros:

- El 94% de las empresas ha sufrido al menos un incidente grave de ciberseguridad a lo largo de 2021 (Fuente Deloitte)
- Los ciberataques durante 2022 han aumentado en un 28% en comparación con 2021 (Fuente Sophos)
- Los ataques de ransomware a pymes fueron los grandes protagonistas, con un incremento del 75% desde el año 2020 (Fuente Sophos)
- Se producen más de 4.000 ataques de ransomware diarios (Fuente F.B.I.)
- En 2022 se registró un aumento del 26% en la cantidad de vulnerabilidades reportadas (el 49% de las empresas confirmó que recibió intentos de ataque que buscaban explotar una vulnerabilidad) (Fuente ESET Security Report)
- El 60% de las empresas tienen más de 500 cuentas con contraseñas que no caducan (Fuente Varonis)
- El 95% de los incidentes de ciberseguridad son producidos por un error humano (Fuente World Economic Forum)
- Los incidentes de ciberseguridad son el riesgo de negocio más importante para 2022 por delante de las pandemias, el cambio climático o los desastres naturales (Fuente Allianz)
- Junto al cambio climático y la desigualdad social, la ciberseguridad es uno de los principales desafíos que enfrenta la humanidad (Fuente World Economic Forum)

ESTRUCTURA ISO 27001:2022

CONTEXTO

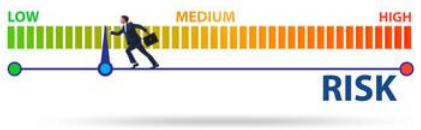
- ❑ Análisis interno y externo de la organización
- ❑ Partes interesadas y sus expectativas
- ❑ Alcance

LIDERAZGO

- ❑ Política de seguridad de la información
- ❑ Objetivos de seguridad de la información
- ❑ Asignación de roles, autoridades, responsabilidades y competencias
- ❑ Disposición de recursos
- ❑ Revisión del sistema por la Dirección

PLANIFICACIÓN - OPERACIÓN

- ❑ Identificación y valoración de activos de información
- ❑ Identificación y valoración de amenazas y vulnerabilidades
- ❑ Identificación y valoración de controles (Anexo A)
- ❑ Plan de tratamiento de riesgos
- ❑ Declaración de aplicabilidad
- ❑ Objetivos
- ❑ Planificación de cambios



SOPORTE

- ❑ Gestión de la información documentada:
  - Identificación, revisión, aprobación y disponibilidad
  - Soporte
  - Protección
  - Cambios
- ❑ RRHH
  - Competencias
  - Plan de formación
  - Sensibilización

EVALUACIÓN DEL DESEMPEÑO

- ❑ Seguimiento y medición - Indicadores
- ❑ Auditoría interna
- ❑ Revisión del sistema por la Dirección

MEJORA

- ❑ No conformidades y acciones correctivas

Intedya
International Dynamic Advisors

93 CONTROLES ANEXO A

Tipo de Control	Propiedades de SI	Conceptos de Ciberseguridad	Capacidad Operativa	Dominios de Seguridad
Preventivo Detectivo Correctivo	Confidencialidad Integridad Disponibilidad	Identificación Protección Detección Respuesta Recuperación	Gobernanza Gestión Activos Seguridad RRHH Seguridad Física Sistemas y redes Seguridad de aplicaciones Configuración segura Gestión de acceso e identidad Gestión de amenazas y vulnerabilidades Continuidad Seguridad en relaciones con proveedores Cumplimiento legal Eventos de seguridad de información Garantía de seguridad de la información	Gobernanza y Ecosistema Protección Defensa Resiliencia

4 grupos

- ORGANIZATIVOS
- PERSONAL
- SEGURIDAD FÍSICA
- TECNOLOGÍA

CONTROLES ANEXO A

GOBERNANZA

- ❑ Políticas específicas
- ❑ Segregación de funciones
- ❑ Contacto con autoridades y grupos de interés

GESTIÓN DE ACTIVOS

- ❑ Reglas de uso aceptable
- ❑ Inventario de activos
- ❑ Asignación de responsables (protección, mantenimiento, gestión, clasificación,…)
- ❑ Devolución de activos
- ❑ Clasificación y etiquetado de la información
- ❑ Soportes extraíbles

SEGURIDAD DE RRHH

- ❑ Antes, durante y después de la relación laboral
- ❑ Cláusulas de confidencialidad
- ❑ Información, concienciación y compromiso con la Política de seguridad
- ❑ Plan de formación
- ❑ Proceso disciplinario
- ❑ Tener en cuenta personal de terceros

CONTROLES ANEXO A

SISTEMAS Y REDES

- ❑ Protección contra interceptación, copia, modificación,…
- ❑ Segregación de redes
- ❑ Acuerdos de intercambio
- ❑ Filtrado web

CONFIGURACIÓN SEGURA

- ❑ Cifrado
- ❑ Plantillas de configuración

SEGURIDAD DE APLICACIONES

- ❑ Limitación y control de instalación se software
- ❑ Pruebas de usabilidad y seguridad
- ❑ Asistencia técnica y actualizaciones de seguridad
- ❑ Evaluación periódica de vulnerabilidades de aplicaciones web
- ❑ Principios de desarrollo seguro con pruebas funcionales y de aceptación
- ❑ Atención a desarrollos subcontratados

SEGURIDAD FÍSICA

- ❑ Perímetro seguro (puertas, ventanas,…)
- ❑ Áreas seguras y de carga/descarga (registro de acceso)
- ❑ Detección/extinción incendios e inundaciones con control de humedad y temperatura
- ❑ Medidas contra cortes eléctricos (SAIs)
- ❑ Activos ubicados fuera de accesos físicos o visuales
- ❑ Mantenimiento
- ❑ Cableado
- ❑ Bloqueo por inactividad
- ❑ Monitorización de la seguridad física

GESTIÓN DE ACCESO E IDENTIDAD

- ❑ Perfiles de usuarios autorizados y permisos (revisión periódica)
- ❑ Principio de mínimo privilegio
- ❑ Usuario y contraseña segura
- ❑ Accesos remotos

CONTROLES ANEXO A

CONTINUIDAD

- ❑ Análisis de impacto de negocio (BIA)
- ❑ Planes de respuesta y recuperación (pruebas periódicas)
- ❑ Preparación de las TIC
- ❑ Redundancias

GESTIÓN DE AMENAZAS Y VULNERABILIDADES

- ❑ Capacidad
- ❑ Antimalware
- ❑ Evaluación de vulnerabilidades
- ❑ Actualizaciones de seguridad
- ❑ Inteligencia de amenazas
- ❑ Sincronización de relojes

SEGURIDAD CON PROVEEDORES

- ❑ Requisitos de seguridad
- ❑ Acuerdos de confidencialidad y SLAs
- ❑ Servicios en la nube

RGPD
REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

CUMPLIMIENTO LEGAL

- ❑ Identificación y cumplimiento de requisitos legales
- ❑ Licencias

EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

- ❑ Recopilación de eventos
- ❑ Gestión, registro y aprendizaje de incidentes de seguridad
- ❑ Monitorización de redes, sistemas y aplicaciones

GARANTÍA DE SEGURIDAD DE LA INFORMACIÓN

- ❑ Evaluación de proveedores
- ❑ Evaluación de vulnerabilidades

ACCIONES A DESARROLLAR

- Designación de **responsabilidades para la protección de activos,** la **gestión de riesgos** y el cumplimiento de las **Políticas.**
- Mantenimiento de **contactos con las autoridades** precisas y los **grupos de interés especial.**
- Definición de políticas y medidas de seguridad para el uso de **dispositivos móviles** y el **teletrabajo.**
- Gestión de **activos** a través de su **inventariado** y la definición de reglas **de uso aceptable.**
- **Clasificación y etiquetado de la información, gestionando el tránsito y la eliminación de soportes extraíbles.**
- Gestión de la relación con los **RRHH** antes, durante y después de la relación laboral.
- **Formación** y **concienciación** de los RRHH.
- Aseguramiento y monitorización de las **instalaciones,** definición de **áreas seguras,** controles de **accesos físicos y** definición de normas para evitar **usos indebidos.**
- Implantación y revisión de sistemas contra **incendios,** contra **inundaciones,** contra **cortes eléctricos,** contra **accesos no autorizados,** etc.…
- Definir procedimientos para la gestión y segregación de las **redes,** y políticas de intercambio de información.

ACCIONES A DESARROLLAR

- **Filtrado web** para limitar la exposición a amenazas y controles de **instalación de software,** con políticas de **desarrollo seguro.**
- Gestión de **vulnerabilidades del sistema y de las aplicaciones web,** con **actualizaciones** de seguridad**.**
- Gestión de los **controles criptográficos** (firmas digitales, certificados, sellos de tiempo, etc…).
- Gestión de **accesos** y procedimientos seguros de **inicio de sesión,** controlando las **autorizaciones** de usuario y definiendo la política de **contraseñas seguras.**
- Supervisión de la **capacidad,** control de **cambios, copias de seguridad,** software **antivirus** y **sincronización de relojes.**
- Auditorías de seguridad con **evaluación de vulnerabilidades.**
- Planificación y prueba de los mecanismos para asegurar la **continuidad de las operaciones,** manteniendo **redundancia** de recursos que asegure la disponibilidad.
- Definición de los requisitos con los **proveedores,** incluyendo **servicios en la nube,** asegurando la **cadena de suministro TIC.**
- Identificación y gestión de los **requisitos legales,** con especial atención a la protección de datos personales y a la propiedad intelectual.
- Monitorización de **eventos** e **incidentes** de seguridad de la información, incluyendo comunicación, evaluación, clasificación, respuesta, aprendizaje y recogida de evidencias.

VENTAJAS ISO 27001:2022

Muchas organizaciones no conocen la información que gestionan o no conocen la importancia de la información que gestionan hasta que se produce una incidencia que les enfrenta a la dura realidad.

Las organizaciones están expuestas a **múltiples amenazas** (fallos energéticos, virus informáticos, fraude, error humano, fallo de elementos, accesos indebidos, desastres naturales, vandalismo, ...) a las que son más o menos vulnerables y para cuya gestión **deben estar preparadas**.

La implantación en las organizaciones de un sistema de gestión de seguridad de la información bajo los requisitos de la **norma ISO/IEC 27001** les permite **minimizar** la probabilidad de materialización de las **amenazas** y estar preparados para minimizar su **impacto** en caso de que se materialicen (pérdidas financieras, litigios laborales, multas, pérdida de clientes, daños de imagen, interrupción de las operaciones, costes de recuperación, ...).

La **norma ISO/IEC 27001** nos lleva a establecer diferentes políticas, procedimientos, aplicaciones informáticas o elementos físicos necesarios para definir la **seguridad de nuestros activos** de manera proporcionada.

"No importa el sector en que opera una organización, que sea grande o pequeña, pública o privada....siempre que disponga de sistemas de información

DEBE PROTEGERSE"

ISO 27001:2022

Sistemas de Gestión de Seguridad de la Información

Área de Seguridad de la Información

Nuestra estrategia,
el DESARROLLO COMPETITIVO.