CRAYON IT CYBERSECURITY

Evaluación ISO/IEC 27001

Alcance

ISO/IEC 27001 es el estándar internacional más reconocido para gestionar la seguridad de la información mediante un Sistema de Gestión de Seguridad de la Información —SGSI—. Su adopción permite a las organizaciones gestionar riesgos sobre información crítica, datos de clientes, propiedad intelectual, continuidad operacional y cumplimiento frente a terceros.

Nuestra evaluación permite identificar qué tan preparada está una empresa respecto al nivel de cumplimiento de ISO/IEC 27001, detectando brechas, controles faltantes, riesgos relevantes y acciones prioritarias para avanzar hacia una implementación sólida, auditable y alineada al negocio.

El resultado es una visión clara del estado actual, el nivel de madurez por dominio y un plan de acción práctico para cerrar brechas antes de iniciar una implementación formal o un proceso de certificación.

DURACION Y MODALIDAD

Duración: 8 semanas

Requiere: Stakeholders del cliente con conocimientos técnicos, estratégicos y operacionales del negocio.

STAKEHOLDERS CLAVE

CEO/Gerencia General, Directorios, CISO/Seguridad de la información, CTO, Riesgo Operacional, Compliance, Auditoría Interna

NUESTRO PROCESO

01 Levantamiento del estado actual

Sesiones con áreas técnicas, áreas de negocio y responsables de seguridad

02 Definición del alcance de evaluación

Identificación del perímetro a evaluar

03 Evaluación de cumplimiento y madurez

Revisión de requisitos ISO/IEC 27001, controles, evidencias y brechas

04 Análisis de riesgos y priorización

Clasificación de hallazgos según criticidad

05 Roadmap de remediación

Diseño de hoja de ruta con quick wins

06 Cierre ejecutivo

CRAYON IT CYBERSECURITY

Evaluación ISO/IEC 27001

Valor para el Negocio

- **Alineado al negocio**
  La evaluación conecta los requisitos de ISO 27001 con procesos críticos, riesgos relevantes y objetivos corporativos.
- **Priorización por riesgo y valor**
  Las decisiones se basan en exposición, impacto, esfuerzo de implementación y capacidad real de ejecución.
- **Quick wins y acciones estructurales**
  Permite identificar mejoras inmediatas sin perder de vista los cambios de gobierno, procesos y tecnología requeridos.
- **Lenguaje ejecutivo**
  Los resultados se presentan en formato comprensible para comités y tomadores de decisión.
- **Base para inversión**
  Cada iniciativa puede ser vinculada a riesgos, beneficios, urgencia y dependencias.

PROBLEMAS QUE RESUELVE

- **Falta de claridad sobre el nivel real de preparación frente a ISO/IEC 27001.**
- **Controles de seguridad implementados de forma aislada, sin conexión con un SGSI.**
- **Dificultad para priorizar iniciativas de seguridad por riesgo, impacto y esfuerzo.**
- **Brechas entre áreas técnicas, procesos internos, gobierno corporativo y objetivos de negocio.**
- **Ausencia de evidencias, políticas, procedimientos o métricas requeridas para una auditoría.**
- **Inversión en tecnología sin una hoja de ruta clara de cumplimiento y madurez.**

CRAYON IT CYBERSECURITY

Evaluación ISO/IEC 27001

Cómo trabajamos

Semana 1: Kick-off y recolección de información

Definición de alcance, objetivos, stakeholders, documentación disponible y contexto organizacional. Revisión inicial de políticas, procesos, activos, arquitectura, herramientas y evidencias.

Semanas 2-3: Levantamiento de negocio y gobierno

Entrevistas con áreas clave para entender procesos críticos, responsabilidades, gestión de riesgos, terceros, continuidad, cultura y prioridades corporativas.

Semana 4-5: Levantamiento técnico y documental

Evaluación de controles existentes, herramientas de seguridad, procesos operacionales, registros, evidencias y capacidades actuales frente a ISO/IEC 27001.

Semanas 6-7: Análisis de brechas, riesgos y madurez

Construcción de matriz de cumplimiento, análisis de brechas, clasificación de hallazgos, evaluación de riesgos y definición de prioridades.

Semana 8: Presentación ejecutiva y roadmap

Entrega de informe final, dashboard, matriz de brechas, roadmap priorizado y presentación ejecutiva con decisiones recomendadas.

ENTREGABLES

- **Informe ejecutivo**
  Resumen de nivel de preparación, principales riesgos, brechas críticas, prioridades y recomendaciones.
- **Matriz de cumplimiento ISO/IEC 27001**
  Evaluación por requisito, dominio y control aplicable, con estado, evidencia, brecha y recomendación.
- **Dashboard de madurez**
  Visualización tipo radar, semáforo o mapa de calor por dominio de evaluación.
- **Matriz de riesgos y brechas**
  Clasificación por criticidad, impacto, probabilidad, esfuerzo y prioridad.
- **Roadmap de remediación**
  Plan de acción con quick wins, iniciativas de corto plazo, proyectos estructurales, responsables sugeridos e hitos.
- **Presentación ejecutiva**
  Material para gerencia, directorio o comité, con decisiones requeridas, prioridades y próximos pasos.
- **Plan de preparación para certificación**
  Recomendaciones para avanzar hacia implementación formal del SGSI, auditoría interna o proceso de certificación.

www.crayonit.com

contacto@crayonit.com

+56 2 3215 1077

linkedin/company/crayonit