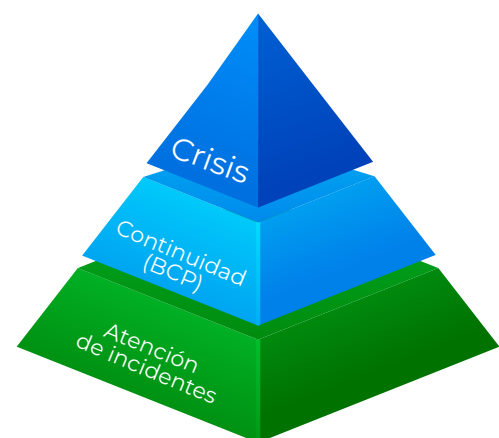


Continuidad de Negocio

Capacidad estratégica y táctica de la organización para responder a incidentes de interrupción con el fin de continuar las operaciones de negocio en niveles aceptables previamente definidos.



Crisis

- Plan de administración y comunicación en crisis

Continuidad

- Planes de Contingencia de Procesos y Tecnología
- Planes de Retorno a la Normalidad

Incidentes

- Planes de Respuesta a Incidentes / Planes de Atención a Emergencias

Seguridad gestionada como un servicio (SMaaS)

Ofrecemos integración durante la implementación del Sistema de Gestión de Seguridad de la información en simultaneo con cuatro servicios:

1. Implementación o alineación con riesgos operativos basados en la norma ISO-31000.
2. Implementación o alineación con continuidad de negocio basados en la norma ISO-22301.
3. Implementación o alineación con buenas prácticas para la gestión de tecnologías de la información basados en gerencia de tecnologías de la información ISO-20000.
4. Monitoreo de eventos e incidentes de su plataforma tecnológica en nuestro SOC.

Estamos ofreciendo prácticamente la estructura de una Dirección de Riesgos (Gestión de riesgo Operativo, Oficial de Cumplimiento, Oficial de Continuidad de Negocio y Oficial de Seguridad Informática en un servicio mensual).



ÉTICA Y TECNOLOGÍA S.A.S.

Soluciones integrales en Seguridad y Gestión de información e infraestructura tecnológica

Mejores prácticas en Ciberseguridad

Identificar:



- Gestión de Activos
- Entorno Empresarial
- Gobernanza
- Evaluación de riesgos
- Estrategia de gestión de riesgos

Detectar:



- Anomalías y eventos
- Monitoreo continuo de la seguridad
- Proceso de detección

Responder:



- Planes de respuesta
- Comunicaciones
- Análisis
- Mitigación
- Mejoras

Proteger:



- Control de acceso
- Capacitación y sensibilización
- Seguridad datos
- Protección información y procedimientos
- Mantenimiento
- Tecnología de protección

Recuperarse:



- Gestión de Activos
- Entorno Empresarial
- Gobernanza
- Evaluación de riesgos
- Estrategia de gestión de riesgos

Contáctenos



3027198995



sandra.caballero@eticaytecnologia.com



www.eticaytecnologia.com

Servicio SaaS para anonimización de datos

Anonimización

La anonimización permite que los datos personales se disocien completamente de los datos identificativos. De esta manera, no es posible relacionar a la persona propietaria de los datos con la información almacenada.

Pseudoanonimización

La pseudoanonimización permite identificar a un sujeto en relación con los datos almacenados sin incluir los datos de la palabra de referencia. Permite el tratamiento de datos personales sin los datos identificativos del interesado, pero sin eliminar el vínculo entre ambos.

Implementación de frameworks

- Sistema de gestion de seguridad de la informacion / ciberseguridad – ISO 27001:2013 / ISO 27032: 2012
- Sistema de gestion de continuidad De negocio – ISO 22301
- Sistema de gestion de riesgos de seguridad de la informacion y ciberseguridad – ISO 31000
- Objetivos de control para la información y tecnologías relacionadas ISO 38500
- Gestión de la infraestructura tecnologica – ISO 20000
- Modelo de seguridad y privacidad de la informacion - MSPI

Apoyamos en la implementación de los siguientes marcos regulatorios:



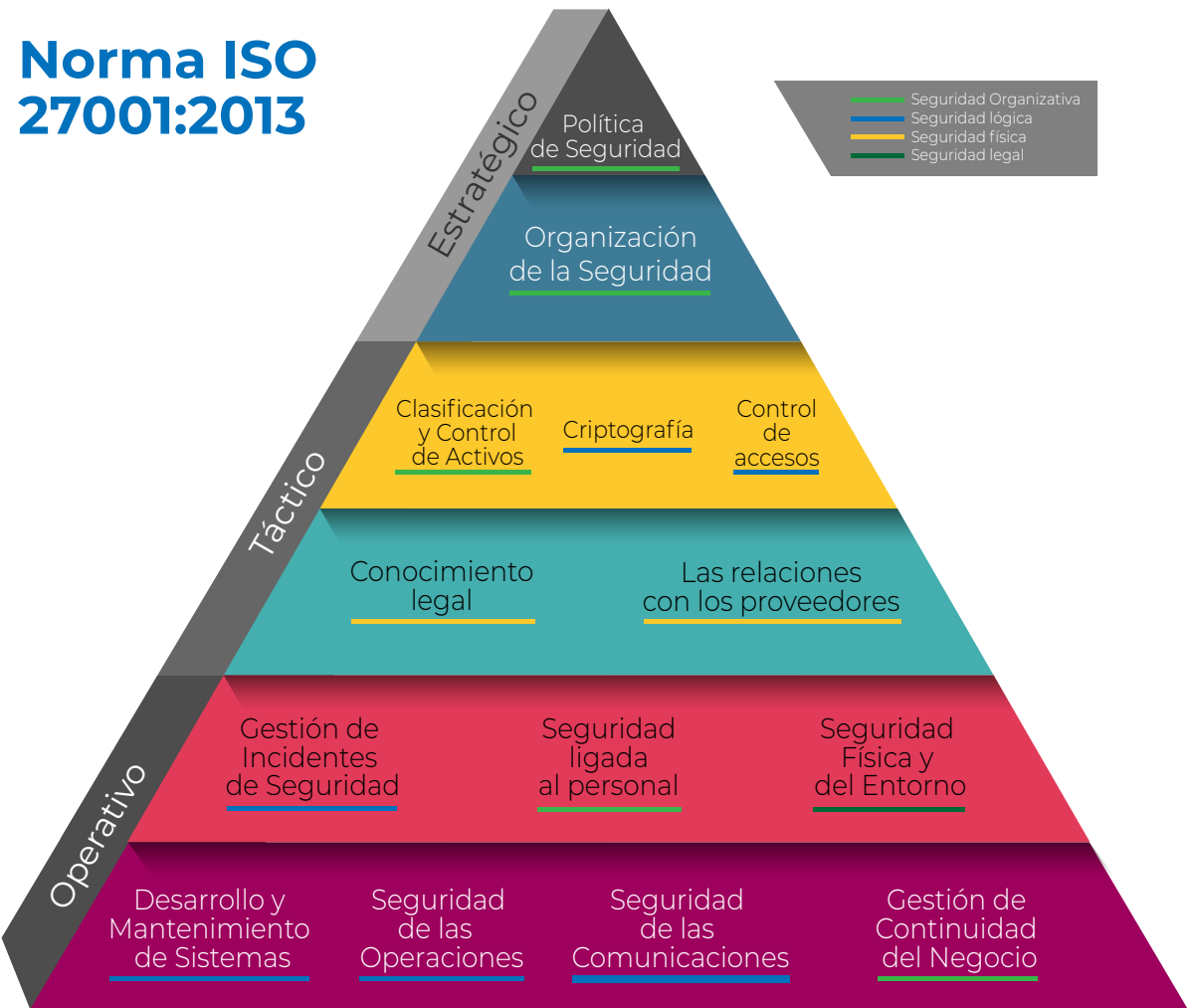
01 Sector privado
LEY 1581 - Protección de datos personales

02 Sector cooperativo
CIRCULAR 36 DE LA SES

03 Sector público
Decreto 2573, Ley 1581, Ley 1712, CONPES 3701 y CONPES 3854
Decreto presidencial 338 de marzo de 2022 - Seguridad Digital

04 Sector financiero
Circular 007, Circular 008, Circular 005 y PCI-DSS
Superintendencia Financiera

Norma ISO 27001:2013



Implementamos sistema de gestión de seguridad de la información bajo ISO/IEC 27002:2022

- A. Atributos
- B. Mapeo a ISO v2013

- 0. Introducción
 - 1. Alcance
 - 2. Referencias
 - 3. Términos y definiciones
 - 4. Estructura Bibliográfica
- 5. Controles organizacionales | 37
- 6. Controles de personas | 8
- 7. Controles físicos | 7
- 8. Controles tecnológicos | 34

Servicio de SOC as a Service



Monitoreo estratégico

La visibilidad contextual dentro de y entre todos los sistemas identifica automáticamente las primeras señales de actividad sospechosa en tiempo real.



Caza de amenazas

Identificación, análisis y mejora de la capacidad de detección mediante una búsqueda exhaustiva entre las actividades maliciosas de ciberamenazas.



Inteligencia de amenazas

Los Indicadores de Compromiso (IOC) continuos basados en información detallada, con herramientas de data que ofrecen alertas proactivas con alto grado de precisión.



Respuesta a incidentes

La respuesta y mitigación en tiempo real en los niveles del 1 al 4 garantizan la más alta protección con el menor impacto en la continuidad del negocio.



Optimización

El continuo desarrollo, aprendizaje de reglas, optimización de correlaciones, actualización de IOC y las nuevas tecnologías de detección maximizan su inversión en ciberseguridad.



Investigación forense

Investigación continua de actividad maliciosa y ciberamenazas potenciales, que incluye análisis post-mortem de incidentes verificados.

Análisis de vulnerabilidades y RED Team

