ACM

Expedient núm. 2024.01

ITGLOBAL

VALUE ON IT

Índex

43519449E DAVID GARCIA (R: B61124376)

Firmado digitalmente por 43519449E DAVID GARCIA (R: B61124376)
Fecha: 2025.05.29 12:19:04 +02'00'

1. Coordinación con la entidad local contratante

Durante toda la prestación del servicio, se establecerá una **coordinación continua y fluida** con la entidad local mediante los siguientes mecanismos:

- **Canal de comunicación dedicado para incidencias**:
  Se habilitará un canal específico e independiente del sistema de monitorización automática (como correo electrónico exclusivo, número de atención directa o plataforma de ticketing). Este canal estará destinado a:
  - Recepción y gestión de incidencias reportadas por el personal de la entidad.
  - Consulta directa con el equipo técnico responsable.
  - Coordinación en tiempo real ante eventos urgentes o críticos.
- **Responsable de interlocución técnica asignado**:
  Se designará una figura de **Responsable de Proyecto** que será el punto de contacto directo con la entidad. Esta persona coordinará las acciones correctivas, revisará los informes y participará en las reuniones periódicas de seguimiento.
- **Reuniones de seguimiento**:
  Se programarán reuniones mensuales (o con la frecuencia que se pacte con la entidad) para:
  - Evaluar la evolución del servicio.
  - Revisar incidentes gestionados y mejoras implementadas.
  - Adaptar el plan de mejora si fuera necesario.

2. Ciberseguridad: Aspectos Clave y Procedimiento ante Desastres

El servicio incluye un enfoque integral de ciberseguridad basado en los siguientes pilares:

Aspectos clave en ciberseguridad:

- Prevención proactiva:

  Implantación de herramientas de detección temprana de amenazas, como firewalls de nueva generación, antivirus avanzados, sistemas EDR (Endpoint Detection & Response), y análisis de tráfico de red con soluciones de NTA (Network Traffic Analysis).

- Segmentación de red y control de accesos:

  Aplicación de políticas de red segmentada (VLANs), gestión de accesos mediante sistemas IAM (Identity and Access Management), y autenticación multifactor (MFA) para accesos críticos.

- Formación y concienciación del personal:

  Programas periódicos de formación para usuarios y personal técnico, simulaciones de ataques tipo phishing y campañas de concienciación adaptadas a los roles dentro de la entidad.

- Actualización continua:

  Uso de herramientas de gestión de parches (patch management), actualizaciones automáticas, y revisión trimestral de los sistemas para asegurar la vigencia de las medidas de protección.

Procedimiento de actuación ante desastres:

Ante un incidente grave (fallo masivo, ataque de ransomware, pérdida de datos, etc.), se seguirá el siguiente protocolo:

1. Activación del plan de respuesta inmediata, incluyendo:
    - Aislamiento del sistema afectado.
    - Notificación inmediata a la entidad local a través del canal de incidencias.
2. Análisis forense inicial:
    - Identificación del origen y alcance del ataque mediante herramientas SIEM (Security Information and Event Management) y software de análisis forense.
    - Evaluación de daños y contención del incidente para evitar su propagación.
3. Ejecución del plan de continuidad del servicio:
    - Restauración de los sistemas mediante copias de seguridad verificadas y testadas previamente.
    - Recuperación escalonada de los servicios críticos y validación de su funcionamiento seguro.
4. Informe post-incidente:
    - Documento detallado con cronología, causas raíz, sistemas afectados, y recomendaciones.
    - Revisión del plan de seguridad y ajustes preventivos para evitar recurrencias.

3. Metodología de Trabajo

El enfoque metodológico para la prestación del servicio se basará en estándares internacionales y buenas prácticas como ISO/IEC 27001, NIST SP 800-53 y el Esquema Nacional de Seguridad (ENS):

1. **Fase de Diagnóstico Inicial**:
   - Revisión documental y técnica de la infraestructura actual.
   - Entrevistas con los responsables TIC de la entidad.
   - Inventario y análisis de activos críticos.
2. **Fase de Auditoría Técnica**:
   - Ejecución de pruebas de vulnerabilidad (internas y externas).
   - Análisis de configuración de servidores, dispositivos de red y sistemas de almacenamiento.
   - Evaluación de los controles actuales frente a estándares de seguridad.
3. **Fase de Diseño del Plan de Mejora**:
   - Priorización de riesgos detectados.
   - Elaboración de una hoja de ruta dividida en fases.
   - Propuestas de medidas técnicas y organizativas (firewalls, cifrado, segmentación, backup, DRP, etc.).
4. **Implementación de mejoras y seguimiento**:
   - Acompañamiento en la puesta en marcha de soluciones.
   - Seguimiento técnico de cada acción implementada.
   - Indicadores de cumplimiento y madurez en ciberseguridad.
5. **Fase de evaluación continua**:
   - Revisiones trimestrales del estado de la infraestructura.
   - Pruebas de restauración y simulacros de recuperación ante desastres.
   - Revisión anual del plan de continuidad del negocio y actualización del plan de contingencia.

4. Marco Normativo y Alineación con Estándares

Este servicio se ajusta a la normativa vigente en materia de protección de datos y ciberseguridad, incluyendo:

- **Esquema Nacional de Seguridad (ENS)**: Se asegura el cumplimiento de los principios básicos y requisitos mínimos exigidos para la protección adecuada de la información tratada por las entidades públicas.
- **Directiva NIS2**: Refuerza la ciberseguridad a nivel europeo, enfocándose en la resiliencia operativa de los servicios esenciales.
- **Reglamento General de Protección de Datos (RGPD)**: Protección de datos personales mediante medidas técnicas y organizativas adecuadas.
- **Normas ISO/IEC 27001, 27002 y NIST 800-53**: Aplicación de buenas prácticas y controles para gestionar la seguridad de la información.
- **Ley 40/2015 de Régimen Jurídico del Sector Público**: Garantiza interoperabilidad, disponibilidad y seguridad en los sistemas de información de la administración pública.

5. Indicadores y Métricas de Seguimiento

Para medir la eficacia del servicio y su evolución a lo largo del tiempo, se establecerán una serie de indicadores clave (KPIs), entre los que se incluyen:

- Número de vulnerabilidades detectadas y mitigadas.
- Tiempo medio de respuesta ante incidentes.
- Porcentaje de cumplimiento del ENS y NIS2.
- Resultados de simulacros y pruebas de restauración.
- Nivel de concienciación del personal (medido mediante test internos).
- Disponibilidad y rendimiento de los sistemas críticos tras implementación.

Estos indicadores se presentarán periódicamente en informes que servirán como base para la toma de decisiones y ajustes en la estrategia de ciberseguridad.

6. Plan de Comunicación y Gestión Documental

- **Informes periódicos**: Documentos mensuales y trimestrales que incluirán estado del sistema, incidencias resueltas, mejoras implementadas y recomendaciones.
- **Actas de reunión**: Recogida formal de decisiones, avances, tareas pendientes y responsables asignados.
- **Repositorio documental**: Plataforma digital con acceso seguro para almacenar políticas, planes, manuales técnicos, copias de seguridad, e historiales de auditoría.
- **Dashboards y paneles de control**: Herramientas visuales en tiempo real para la supervisión continua del estado de la infraestructura.

7. Beneficios Esperados y Compromiso con la Mejora Continua

La prestación de este servicio reportará a la entidad local importantes beneficios tangibles e intangibles:

- Fortalecimiento de la infraestructura tecnológica y mayor capacidad de respuesta ante ciberamenazas.
- Cumplimiento riguroso de las normativas en vigor, minimizando riesgos legales y reputacionales.
- Mayor eficiencia operativa y reducción del tiempo de inactividad de los sistemas críticos.
- Formación continua que refuerza la cultura de seguridad dentro de la organización.
- Mejora progresiva basada en evaluaciones periódicas y revisión constante de los mecanismos de protección.

Este compromiso con la mejora continua garantiza no solo una respuesta eficaz ante el presente, sino una preparación adecuada para los retos futuros en materia de ciberseguridad.