Tabla de contenidos

Colombian Tech & Consulting SAS establece los siguientes Acuerdos de Nivel de Servicio (SLAs) para garantizar la calidad, disponibilidad y tiempos de respuesta de los servicios de SOC, NOC, MDR y Help Desk. Este documento unifica los estándares aplicables a todos los servicios, priorizando la claridad y la eficiencia en la gestión de incidentes y solicitudes.

1. Clasificación de niveles de criticidad

Para todos los servicios, los incidentes y alertas se clasifican en los siguientes niveles de criticidad:

1.1. Crítico (Prioridad Urgente)

- Descripción: Amenazas o problemas que impactan de forma grave la continuidad operativa, disponibilidad o seguridad de sistemas críticos.
- Ejemplos:
    - Caída total de la red o sistemas críticos (SOC/NOC).
    - Malware activo, como ransomware (SOC/MDR).
    - Fallo en herramientas esenciales para la operación del cliente (Help Desk).
- Tiempo de respuesta: Notificación al cliente en menos de 15 minutos.
- Acción: Escalamiento inmediato y seguimiento continuo hasta la contención y/o remediación.

1.2. Alto (Prioridad Alta)

- Descripción: Alertas sospechosas o fallos con potencial de convertirse en críticos si no se abordan rápidamente.
- Ejemplos:

- Intentos de fuerza bruta o anomalías en configuraciones críticas (SOC/MDR).
- Latencia alta en enlaces clave o degradación del rendimiento de sistemas (NOC).
- Problemas con aplicaciones secundarias pero necesarias para el trabajo diario (Help Desk).

- Tiempo de respuesta: Notificación al cliente en menos de 30 minutos.
- Acción: Revisión y seguimiento inicial en 2 horas.

1.3. Medio (Prioridad Media)

- Descripción: Incidentes menores que no afectan de forma inmediata las operaciones, pero requieren atención para prevenir problemas futuros.
- Ejemplos:
  - Dispositivos con configuraciones subóptimas o software desactualizado (SOC/NOC/MDR).
  - Solicitudes de configuración no urgentes (MDR/Help Desk).
- Tiempo de respuesta: Notificación al cliente en menos de 4 horas.
- Acción: Resolución o recomendaciones dentro de 1 día hábil.

1.4. Bajo (Prioridad Baja)

- Descripción: Alertas menores, eventos esperados o problemas secundarios que no impactan la operación del cliente.
- Ejemplos:

- Notificaciones de actividades rutinarias o cambios en el entorno (SOC/NOC).
- Revisión de configuraciones en dispositivos no críticos (MDR/NOC).

- Tiempo de respuesta: Notificación dentro de 1 día hábil.
- Acción: Seguimiento según cronograma acordado.

1.5. Informativo

- Descripción: Eventos registrados como referencia para análisis futuro; no requieren acción inmediata.
- Ejemplos:
  - Backups completados, cambios programados exitosos (SOC/NOC/MDR).
  - Incrementos esperados en tráfico o actividad de usuarios (NOC).
- Acción: Registro y análisis en informes periódicos.

2. Disponibilidad del servicio

Se contemplan los siguientes porcentajes de disponibilidad para todos los servicios (SOC, NOC, MDR y Help Desk):

- Modalidad 8x5: 99.5% de disponibilidad durante el horario laboral contratado.
- Modalidad 24x7: 99.9% de disponibilidad ininterrumpida.

3. Reportes y comunicación

- Frecuencia: Diarios, semanales o mensuales según contrato.

- Contenido:
    - Resumen de incidentes y alertas por niveles de criticidad.
    - Tiempos de respuesta y acciones realizadas.
    - Recomendaciones para optimizar la operación y seguridad.

4. Condiciones y exclusiones

4.1. Activación de los tiempos de respuesta

- Los tiempos comienzan al detectar el incidente o recibir la solicitud a través de los canales designados (correo electrónico, línea directa, portal de soporte).

4.2. Exclusiones

- Fallos fuera del alcance del servicio, como problemas en sistemas no gestionados por Colombian Tech & Consulting SAS.
- Casos de fuerza mayor o interrupciones por terceros.

4.3. Responsabilidad del cliente

- Proveer acceso adecuado a las herramientas, plataformas y sistemas monitoreados.
- Implementar las recomendaciones proporcionadas por nuestro equipo.