Protocolo de Seguridad para las Plataformas LMS del Consorcio Advance – Contrato 381-2025

Este documento detalla el **Protocolo de Seguridad de las Plataformas LMS** del **Consorcio Advance – Contrato 381-2025**, una guía esencial para gestionar de manera efectiva cualquier interrupción en la disponibilidad de nuestra plataforma de educación virtual. Su propósito es garantizar la disponibilidad, confidencialidad e integridad de la información y garantizar una respuesta rápida, coordinada y transparente a los requerimientos o incidentes del servicio, minimizando el impacto en los usuarios y facilitando una recuperación eficiente y el aprendizaje continuo.

1. Objetivo Principal

El objetivo primordial de este protocolo es establecer un marco de acción claro y conciso para la **detección, gestión, resolución y comunicación** de incidentes que afecten la disponibilidad, confidencialidad e integridad de la información almacenada en nuestra plataforma de educación virtual. Buscamos:

- **Minimizar el tiempo de inactividad (Downtime):** Reducir al máximo el período durante el cual la plataforma no está operativa.
- **Reducir el impacto en el usuario:** Limitar la afectación a la experiencia del usuario y la pérdida de funcionalidad.
- **Asegurar la integridad de los datos:** Proteger la información y minimizar cualquier potencial pérdida.
- **Facilitar una recuperación rápida y eficiente:** Restaurar los servicios a su estado normal de operación en el menor tiempo posible.
- **Fomentar la mejora continua:** Aprender de cada incidente para fortalecer la resiliencia de la plataforma.

2. Alcance del Protocolo

Este protocolo es de aplicación obligatoria para todos los equipos y personal involucrado directa o indirectamente en la operación, mantenimiento y soporte de la plataforma. Esto incluye, pero no se limita a:

- Equipos de Operaciones y Soporte Técnico.
- Equipos de Producto y Gestión de Proyectos.
- Equipos de Comunicaciones y Marketing.

3. Definiciones Clave

Para una comprensión uniforme y sin ambigüedades:

- **Indisponibilidad:** Estado en el cual las plataformas web, o una de sus funcionalidades críticas, no es accesible o no funciona correctamente para un segmento significativo de usuarios.
- **Incidente Crítico (Sev1 - Severidad 1):** Indisponibilidad total de la plataforma web o de una funcionalidad central que impide la operación normal del negocio y afecta a la mayoría o la totalidad de los usuarios. Requiere respuesta inmediata 24/7.
- **Incidente Mayor (Sev2 - Severidad 2):** Indisponibilidad parcial o degradación significativa del rendimiento que afecta a un subconjunto considerable de usuarios o funcionalidades no críticas, pero que impacta la experiencia del usuario o la operación.
- **Tiempo Objetivo de Recuperación (RTO - Recovery Time Objective):** El tiempo máximo aceptable para restaurar la plataforma a un estado operativo después de un incidente.
- **Punto Objetivo de Recuperación (RPO - Recovery Point Objective):** La cantidad máxima de datos que se está dispuesto a perder (medido en tiempo) desde el momento de la indisponibilidad hasta la recuperación.
- **Causa Raíz:** El factor fundamental que, al eliminarse, previene la recurrencia de un problema.

4. Roles y Responsabilidades

La claridad en los roles es crucial para una respuesta eficaz y sin fricciones:

- **Equipo Técnico de Respuesta:**
  - **Responsabilidad:** Diagnosticar, mitigar y resolver el incidente.
  - **Funciones:** Investigar la causa raíz, implementar soluciones, monitorear el impacto de las acciones y validar la restauración del servicio.

- **Equipo de Comunicaciones/Soporte:**
  - **Responsabilidad:** Gestionar la comunicación con los usuarios, clientes y stakeholders externos.
  - **Funciones:** Publicar actualizaciones en la página de estado, redes sociales y otros canales, responder a consultas de usuarios y escalar información relevante al equipo técnico.
- **Stakeholders (Gerencia/Dirección):**
  - **Responsabilidad:** Estar informados sobre el progreso del incidente y tomar decisiones estratégicas si es necesario.
  - **Funciones:** Recibir actualizaciones periódicas del IC, aprobar recursos adicionales o cambios de estrategia si el incidente es prolongado o de alto impacto.

5. Fases del Protocolo de Indisponibilidad

5.1. Fase 1: Detección y Notificación Inicial

a. **Monitoreo Proactivo:**
   - Alertas configuradas para notificar automáticamente al equipo de guardia (on-call).

b. **Reporte de Usuarios/Clientes:**
   - Canales de soporte (tickets, llamadas, chat, etc.) donde los usuarios pueden reportar problemas.

c. **Verificación y Confirmación:**
   - El equipo de guardia verifica la alerta o el reporte (ej. intentando acceder a la plataforma, revisando logs).
   - Se determina el alcance inicial y el impacto percibido (ej. ¿es un usuario o muchos? ¿Qué funcionalidad está afectada?).

d. **Activación del Protocolo:**
   - Si se confirma una indisponibilidad, el equipo de guardia notifica inmediatamente al equipo técnico a través de los canales de comunicación de emergencia (Llamada, WhatsApp, tickets, SMS).

5.2. Fase 2: Evaluación y Clasificación del Incidente

a. **Reunión de Crisis Inicial (War Room):**
   - El agente que detecto el incidente convoca una llamada de conferencia inmediata (Telefónica, Meet, WhatsApp) con el equipo técnico clave.
   - **Clasificación de Severidad:** Se clasifica el incidente como **Sev1** o **Sev2** basándose en

el impacto real en los usuarios y el negocio.

- **Hipótesis Iniciales:** Se comparten las primeras hipótesis sobre la causa y se identifican los sistemas potencialmente afectados.
- **Confirmación de RTO y RPO:** Se reafirman los objetivos de recuperación para este incidente específico.

b. **Establecimiento de un Canal de Comunicación Dedicado:**

- En el canal de chat específico para todas las comunicaciones internas relacionadas con el incidente.

5.3. Fase 3: Diagnóstico y Resolución

1. **Investigación y Recopilación de Información:**
   - El equipo técnico profundiza en la investigación, revisando logs de aplicaciones y sistemas, métricas de rendimiento, configuraciones recientes, estado de servicios y cualquier cambio o despliegue reciente.
2. **Identificación de la Causa Raíz (o Mitigación Rápida):**
   - Se formulan hipótesis sobre la causa y se realizan pruebas controladas para confirmarlas o descartarlas.
   - Se asignan tareas claras y responsables a los miembros del equipo.
3. **Ejecución y Monitoreo Continuo:**
   - El equipo ejecuta las acciones del plan de forma coordinada.
   - Cada acción es monitoreada en tiempo real para observar su impacto y asegurar que no se introduzcan nuevos problemas.
4. **Validación de la Solución:**
   - Una vez implementada la solución, se realizan pruebas de funcionalidad completas para confirmar que el servicio ha sido restaurado y opera normalmente desde la perspectiva del usuario.

5.4. Fase 4: Comunicación durante el Incidente

a. **Comunicación Interna:**

- El equipo técnico proporciona actualizaciones regulares al equipo técnico y a las directivas a través del canal de chat del incidente y/o llamadas de actualización.
- **Actualizaciones Periódicas:** Se proporcionarán actualizaciones regulares sobre el progreso en la resolución del incidente, incluso si no hay avances significativos. La transparencia es clave.
- **Notificación de Resolución:** Una vez que el servicio ha sido completamente restaurado y validado, se envía una comunicación final a todos los canales informando sobre la

resolución del incidente y agradeciendo la paciencia.

5.5. Fase 5: Post-Incidente y Mejora Continua

a. **Monitoreo Intensivo Post-Resolución:**
   - Durante un período definido después de la resolución, la plataforma debe ser monitoreada de forma más intensiva para asegurar su estabilidad a largo plazo y detectar cualquier posible recurrencia o efecto secundario.

b. **Comunicación de Cierre:**
   - El equipo técnico o el equipo de comunicaciones envía un comunicado final a todos los stakeholders internos y externos afectados, resumiendo el incidente y confirmando la resolución definitiva.

6. Canales de Comunicación durante un Incidente

- **Internos:**
  - **Chat:** Teams Chat, grupo de WhatsApp.
  - **Llamadas de Conferencia:** Teams.

7. Anexos y Documentación Complementaria

- **Lista de Contactos de Emergencia:** Números de teléfono y correos electrónicos actualizados de los miembros clave del equipo y proveedores de servicios críticos.
- **Guía de Escalada:** Criterios y pasos para escalar un incidente a niveles superiores de gestión o a proveedores externos.

ADVANCE Consortium