GLI-CMP
PROGRAMA DE GESTIÓN DEL CAMBIO

GUÍA

PARA LOS SISTEMAS DE LA INDUSTRIA DEL JUEGO

Versión 1.0 - Publicada el 6 de mayo de 2020

Contenido

1. INTRODUCCIÓN

1.1. Alcance

Proporcionar una guía de mejores prácticas en la implementación de un Programa de Gestión del Cambio (CMP de aquí en adelante) para permitir la Entrega Continua, el Desarrollo Ágil o prácticas similares que se emplean como estándar de la industria en las compañías de tecnología que operan en línea o con plataformas muy diversas. El CMP debe ampliar la aplicación de la supervisión y la gobernanza reglamentarias adecuadas, modernizando al mismo tiempo el enfoque del proceso de cumplimiento regulatorio para satisfacer las demandas de las nuevas ofertas de tecnología. El objetivo del presente documento es elaborar un marco de criterios coherentes y uniformes para la industria en lo que respecta a la aplicación de un CMP que permita el crecimiento, la innovación y la eficiencia en función de los costos en el proceso de desarrollo que rivaliza con las industrias no relacionadas con el juego. Al mismo tiempo, el proceso de CMP debe construirse de manera que se mantenga el enfoque en la protección de la integridad del juego y la confianza en todas las instituciones de buena fe en el marco de la actual arquitectura de supervisión regulatoria

La orientación proporcionada por el presente documento tiene por objeto aclarar lo siguiente a los operadores autorizados, sus proveedores de tecnología y los laboratorios de pruebas independientes.

a. Criterios mínimos para la elaboración de una política oficial de gestión del cambio a nivel de organización;
b. Directrices para la aplicación y el funcionamiento en el marco del programa de gestión del cambio; y
c. Procedimientos, formato y requisitos de archivo uniformes mínimos para que toda la información sea registrada por un Programa de Gestión del Cambio.

1.2. Estándares consultados

La presente guía se ha elaborado mediante el examen y la utilización de partes de los siguientes documentos:

a. Dinamarca - Programa de certificación de Spillemyndigheden Programa de gestión del cambio SCP.06.00
b. Suecia - Reglamento y directrices generales de la Inspección de Loterías sobre los requisitos técnicos y la acreditación de los organismos que realizan la inspección, ensayo y certificación de las actividades de juego (LIFS 2018_8)
c. Portugal - Reglamento N°903-B/2015 Reglamento p or el que se definen los requisitos técnicos del sistema técnico de juegos en línea
d. Reino Unido - Estrategia de ensayos para el cumplimiento de las normas técnicas de juego remoto y software Noviembre de 2018 y auditoría anual de ensayos de los Juegos - Plantilla Junio de 2018
e. Indiana - Directiva de Gestión del Cambio
f. Iowa - 491-13.6(99F) Pruebas. 13.6(2) Control de cambios

1.3. Necesidad

Las plataformas modernas requieren una vigilancia de la vulnerabilidad o los errores que se originan por la exposición a amenazas continuas por medio de ataques, aumento de la carga y/o interacción con hardware, componentes de red o sistemas operativos y software complementario que se actualizan constantemente. Esto puede ser cierto tanto si se opera en línea como si se utiliza una plataforma para gestionar una o más partes de una operación en un entorno de red cerrado. Ambos tipos de despliegues están expuestos a estas mismas amenazas.

Los sistemas modernos contrarrestan estas amenazas a través de técnicas para desarrollar código en pequeños y eficientes ciclos para mantenerse al tanto de la evolución del entorno. Estas técnicas están

diseñadas para proporcionar una mayor fiabilidad, productividad y calidad general, pero existen obstáculos para este enfoque en mercados altamente regulados como el de los juegos de azar, en el que se requieren pruebas exhaustivas antes de cada lanzamiento. El objetivo no es eliminar la supervisión y las pruebas del proceso, sino alinearse de tal manera que las operaciones de juego puedan funcionar como otras operaciones de comercio electrónico para garantizar un entorno seguro y estable con las más recientes características de las operaciones en industrias paralelas.

2. CERTIFICACIÓN

2.1. Certificación Inicial

El operador con licencia y el proveedor de tecnología, cuando estén separados, son responsables de asegurar que todos los productos implementados en las jurisdicciones de juego estén certificados de conformidad con las normas y reglamentos de las jurisdicciones y vayan acompañados de una documentación de certificación formal que indique como tal.

2.2. Certificación Annual

A menos que el órgano regulador especifique lo contrario, una vez al año como mínimo, cada producto que funcione en el marco de un programa de gestión del cambio debe estar plenamente certificado con arreglo a las normas y reglamentos de todas las jurisdicciones que operen en este y debe ir acompañado de documentación de certificación oficial de un laboratorio de pruebas independiente que conozca el producto. El operador autorizado y el proveedor de tecnología, cuando sean independientes, podrán solicitar la aprobación de la extensión de la aprobación anual si se puede demostrar que existen dificultades. La concesión de una exención por dificultades es a discreción exclusiva del organismo regulador.

2.3. Certificación de gestión del cambio

A menos que el órgano regulador especifique de otra forma, las políticas y procedimientos de gestión del cambio elaborados de conformidad con la presente guía serán aprobados por el órgano regulador antes de la implantación del CMP y auditados a intervalos anuales por el laboratorio de pruebas independiente.

2.4. Informes de cambio trimestrales

A menos que el órgano regulador especifique lo contrario, se emiten informes trimestrales a un laboratorio de pruebas independiente con conocimiento del producto para su revisión, a fin de garantizar que el riesgo se evalúa de acuerdo con el CMP certificado y que toda la documentación de todos los cambios está completa. El laboratorio de ensayo independiente evaluador elaborará un informe oficial en el que se indicará que la revisión es completa.

2.5. Auditorías de seguridad

A menos que el órgano regulador especifique lo contrario, se realizará una auditoría de seguridad anual para complementar las pruebas y la certificación anual designadas en la sección 2.2. La auditoría de seguridad cubre el sistema operativo subyacente, el componente de red y los cambios de hardware no incluidos en la evaluación del software de juego recalificado según la sección 2.2.

3. POLÍTICA Y PROCEDIMIENTOS DE GESTIÓN DEL CAMBIO

3.1. Directrices

El operador con licencia y/o el proveedor de tecnología deberá presentar documentación que describa los procesos y procedimientos de control de cambios que se van a desplegar dentro de la organización y a los que se va a adherir, cubriendo todos los pasos del despliegue, desde el desarrollo inicial hasta el desarrollo de los controles de procesos y versiones del código fuente, pasando por las pruebas internas y la aprobación del despliegue. Se espera que los procesos y procedimientos de control de cambios se redacten específicamente según el enfoque del operador autorizado y/o el proveedor de tecnología con respecto al ciclo de vida del desarrollo, pero que incluyan como mínimo la cobertura de lo siguiente:
a. La adquisición y el desarrollo de nuevos componentes de software y/o hardware;
b. Un control o mecanismo de versión de software apropiado para todos los componentes de software, código fuente y controles binarios;
c. Normas y prácticas de codificación utilizadas por la organización;
d. Normas y prácticas de ensayo internas utilizadas por la organización, incluidos los métodos documentados para:
    i. Asegurar que los datos de producción en bruto no se utilicen en los ensayos;
    ii. Verificar que el software de prueba no se despliegue en el entorno de producción;
e. Separación del entorno de producción de los entornos de desarrollo y de prueba, tanto lógica como físicamente. Cuando se utilizan plataformas de nubes, no puede existir una conexión directa entre el entorno de producción y cualquier otro entorno;
f. Separación de las tareas dentro del proceso de lanzamiento;
g. Si aplica, establecer la delegación de responsabilidades entre el operador licenciado y/o el proveedor de tecnología;
h. Procedimientos para la migración de los cambios para garantizar que sólo se implementen en el entorno de producción los componentes autorizados;
i. Una estrategia para cubrir la posibilidad de una instalación fallida o un problema de campo con uno o más cambios implementados en el marco del CMP:
    i. Cuando una parte externa, como una tienda de aplicaciones, sea parte interesada en el proceso de lanzamiento, esta estrategia debe cubrir la gestión de los lanzamientos a través de la parte externa. Esta estrategia puede tener en cuenta la gravedad del problema;
    ii. En caso contrario, esta estrategia debe abarcar la vuelta a la última implementación (plan de retroceso), incluyendo copias de seguridad completas de las versiones anteriores del software y una prueba del plan de retroceso antes de la implementación en el entorno de producción;
j. Una política que aborde los procedimientos de cambio de emergencia;
k. Toda la documentación relativa al desarrollo del software y aplicaciones, incluidos los procedimientos para garantizar que la documentación técnica y de usuario se actualice como resultado de un cambio; y
l. Identificación de personas con licencia para su aprobación antes del lanzamiento.

4. REGISTRO DE ACTIVOS CRÍTICOS (CAR)

4.1. Clasificación de Componentes

4.1.1. Criterios de clasificación

El proveedor de tecnología clasificará todos los componentes de la plataforma o producto operado bajo el CMP con arreglo a los cuatro criterios siguientes:
a. Confidencialidad - Información confidencial relacionada con los jugadores de la plataforma. Por ejemplo, la identificación/información personal de un jugador en el sistema o la información transaccional de los datos de los jugadores.

b. Integridad - La integridad de la plataforma, específicamente cualquier componente que afecte a la funcionalidad de la plataforma o que influya en la forma en que la plataforma almacena/maneja la información.

c. Disponibilidad - La disponibilidad de la información de los jugadores.

d. Contabilidad - La actividad del usuario, y en qué medida influye el componente en cuestión en la actividad del usuario.

4.1.2. Código de relevancia

A cada componente se le asignará un código de relevancia en la escala que se indica a continuación, en base de la función del componente en el logro o la garantía de cada uno de los criterios de clasificación anteriores:
a. 1 - Ninguna relevancia (el componente no puede tener un impacto negativo en los criterios);
b. 2 - Cierta relevancia (el componente puede tener un impacto en los criterios); y
c. 3 - Relevancia sustancial (los criterios están relacionados o dependen del componente).

4.2. Registro de los componentes en un CAR

Todos los componentes definidos serán registrados en un Registro de Activos Críticos (CAR de aquí en adelante). La estructura del registro de componentes incluirá los componentes de hardware y software y las interconexiones y dependencias de los componentes. Se documentarán los siguientes elementos mínimos para cada componente:
a. El nombre/definición de cada componente;
b. Una identificación única que se asigna a cada componente individual;
c. Un número de versión del componente listado;
d. Características de identificación (Componente de la plataforma, Base de datos, Máquina Virtual, Hardware);
e. El propietario responsable del componente;
f. La ubicación geográfica de los componentes de hardware; y
g. Códigos de relevancia sobre los criterios de clasificación:
    i. Confidencialidad
    ii. Integridad
    iii. Disponibilidad
    iv. Contabilidad

4.3. Lista de verificación del programa de control

El proveedor de tecnología proporcionará un informe de todos los archivos de software identificados como componentes críticos del programa de control junto con las correspondientes firmas digitales del componente o componentes críticos del programa de control; como mínimo, las firmas digitales deberán emplear un algoritmo criptográfico que produzca un resumen de mensajes de al menos 128 bits.

5. REGISTRO DE GESTIÓN DEL CAMBIO (CML)

5.1. Clasificación de los cambios

5.1.1. Nivel 1 - Sin impacto

El cambio no afecta a los componentes regulados de la plataforma.
Ejemplos:
a. Instalación o cambios en los componentes de software y/o hardware de respaldo;
b. Adición o eliminación de usuarios;
c. Mantenimiento de la base de datos que modifique o elimine datos no críticos de la base de datos.
d. Interrupciones programadas o mantenimiento de cualquier infraestructura de proveedor de servicios de red;

e. Interrupciones programadas o mantenimiento de cualquier infraestructura eléctrica (generador, ATS, UPS, PDU, etc.); o
f. Instalación de parches de seguridad del sistema operativo
g. Imágenes de fondo, esquemas de color, o similares actualizaciones auxiliares del frente al cliente.

5.1.2. Nivel 2 - Bajo impacto

El cambio tiene un bajo impacto en la integridad de la plataforma. Esto también puede incluir cambios en los componentes del hardware.
Ejemplos
a. Cambios en las reglas del cortafuegos;
b. Mantenimiento de la base de datos;
c. Cambios en la ubicación física de los datos primarios de respaldo regulados;
d. Cualquier cambio o adición de un componente físico de hardware; o
e. Cambios en los componentes lógicos no relacionados con el juego de la plataforma principal que no sean de carácter benigno, como se describe para el Nivel 1 y con la excepción de los ejemplos representativos de los cambios del Nivel 3.

5.1.3. Nivel 3 - Alto Impacto

El cambio tiene un gran impacto en los componentes regulados o en la presentación de informes de la plataforma.
Ejemplos:
a. Implementación de una nueva característica de juego o un cambio en cualquier lógica que afecte las apuestas o la lógica del juego;
b. Un cambio que afecte los informes reglamentarios requeridos o los datos utilizados para la conciliación financiera;
c. Si es aplicable, un cambio implementado por el proveedor de la plataforma que impacte sustancialmente en los servicios de geolocalización;
d. Si es aplicable, un cambio que afecte al manejo o almacenamiento de información de identificación personal; o
e. Un cambio para incorporar los requisitos reglamentarios actualizados.

5.2. Criterios mínimos de registro

Todos los cambios deben ser documentados en el CML. El proveedor de tecnología registrará las instalaciones y/o modificaciones de la plataforma en el CML. Es responsabilidad del proveedor de la plataforma crear y mantener el CML. El CML registrará como mínimo lo siguiente:
a. Fecha y hora en que se aprueba internamente un cambio para su inplementación;
b. El componente o componentes que se van a modificar, incluido el número de identificación único del CAR, la información de la versión;
c. Detalles del motivo o la característica de la instalación o el cambio, como nuevo software, reparación del servidor, modificación significativa de la configuración. Si el componente que se va a cambiar es un componente de hardware, la ubicación física de este componente de hardware;
d. Identificación de la persona responsable de autorizar el cambio;
e. Identificación de la persona que realiza el cambio;
f. Fecha prevista de lanzamiento de la instalación o modificación; y
g. El nivel del cambio (Nivel 1, 2, o 3).

6. GESTIÓN DE CAMBIOS DE NIVEL 2 Y NIVEL 3

6.1. Notificación

Para los cambios de Nivel 2 o Nivel 3, se debe dar un aviso previo de al menos 3 días hábiles antes del despliegue a los organismos reguladores y al laboratorio de pruebas independiente que realizó la certificación previa. Los organismos reguladores o el laboratorio de pruebas independiente, si así lo delegan los organismos reguladores, se reservan el derecho de solicitar la prueba y, potencialmente, la certificación de las actualizaciones de la plataforma antes de su implementación. Si la política reglamentaria no designa normas adicionales para la gestión de los cambios de nivel 2 o 3 y no se notifica el requisito de realizar pruebas adicionales en un plazo de 3 días hábiles, se concede una aprobación pasiva por la que se aprueba al operador autorizado y/o al proveedor de tecnología para introducir el cambio en la producción. Los procedimientos de notificación se manejarán según cada jurisdicción.

6.1.1. Atestación

En la notificación del despliegue de cualquier cambio se incluirá un certificado de confirmación de buena fe, basado en las prácticas y normas internas de desarrollo y ensayo, de que los cambios que se están introduciendo cumplen con todas las leyes, reglas y reglamentos de cada jurisdicción.

6.1.2. Lista de verificación del programa de control

En la notificación de despliegue de cualquier cambio en un componente crítico del programa de control se incluirá un informe de la Lista de Verificación del Programa de Control que detalla todos los componentes de control de la plataforma y su correspondiente firma digital más reciente.

6.2. Prueba de los cambios.

6.2.1. Pruebas antes del despliegue

En caso de que sea necesario certificar los cambios de nivel 2 y 3 antes de su despliegue, las pruebas de laboratorio de esos cambios se certificarán de conformidad con las normas y reglamentos de todas las jurisdicciones que operen en ellas y se acompañarán de la documentación de certificación formal de un laboratorio de pruebas independiente con conocimiento del producto.

6.2.2. Pruebas después del despliegue

En los casos en que no sea necesario certificar los cambios de nivel 2 y 3 antes de su despliegue, las pruebas de laboratorio de estos cambios se completarán en un plazo de 90 días a partir de su introducción en el entorno de producción. El proceso de ensayos no impedirá que el operador autorizado o el proveedor de tecnología continúe desarrollando e introduciendo cambios en el marco del programa de gestión de cambios. El establecimiento del CMP permitirá la notificación de los hallazgos resultantes de cada ciclo de pruebas, que se notificarán mediante estructuras acordadas con cada organismo regulador.

6.2.3. Exenciones por dificultades

El proveedor de tecnología podrá solicitar la aprobación de una extensión de más de 90 días si se demuestra que existen dificultades. La concesión de una exención por dificultades es a discreción exclusiva del organismo regulador.

6.3. Regla de emergencia

En situaciones de emergencia para hacer frente a amenazas o contingencias pendientes, un operador con licencia o un proveedor de tecnología puede ejecutar inmediatamente cambios de nivel 2 o 3 sin consentimiento previo. Se notificará a los órganos reguladores lo antes posible y de conformidad con las normas de emergencia establecidas. La notificación incluirá la necesidad de emplear la regla de emergencia y todos los detalles conocidos en ese momento sobre la actualización necesaria. Los órganos reguladores se reservarán el derecho de realizar análisis en cada caso de emergencia para verificar la necesidad de las medidas adoptadas.