centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1229

Procedimiento de empleo seguro
Microsoft Sentinel

Abril 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid.

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.04.12 09:39:06 +02'00'

NIPO: 083-24-145-4.
Fecha de Edición: abril 2024.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

ÍNDICE **2**
1. INTRODUCCIÓN **3**
2. OBJETO Y ALCANCE **4**
3. ORGANIZACIÓN DEL DOCUMENTO **5**
4. FASE PREVIA A LA INSTALACIÓN **6**
4.1 ENTREGA SEGURA DEL SERVICIO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 REGISTRO Y LICENCIAS 6
4.4 CONSIDERACIONES PREVIAS 6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 6
5. FASE DE INSTALACIÓN **8**
5.1 ALTA DEL SERVICIO EN LA NUBE 8
5.2 DESPLIEGUE DE MICROSOFT SENTINEL 8
6. FASE DE CONFIGURACIÓN **9**
6.1 MODO DE OPERACIÓN SEGURO 9
6.2 AUTENTICACIÓN 9
6.3 ADMINISTRACIÓN DEL SERVICIO 10
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 10
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 10
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 11
6.5 GESTIÓN DE CERTIFICADOS 12
6.6 SERVIDORES DE AUTENTICACIÓN 12
6.7 SINCRONIZACIÓN 12
6.8 ACTUALIZACIONES 12
6.9 ALTA DISPONIBILIDAD 12
6.10 AUDITORÍA 12
6.10.1 REGISTRO DE EVENTOS 12
6.10.2 ALMACENAMIENTO LOCAL 13
6.10.3 ALMACENAMIENTO REMOTO 13
6.11 BACKUP 14
6.12 FUNCIONES DE SEGURIDAD 14
7. FASE DE OPERACIÓN **15**
8. REFERENCIAS **16**
9. ABREVIATURAS **17**

1. INTRODUCCIÓN

1. Microsoft Sentinel es una solución escalable y nativa en la nube que proporciona:
    - Administración de eventos e información de seguridad (SIEM)
    - Respuesta automatizada de orquestación de seguridad (SOAR)
2. Microsoft Sentinel se utiliza para proporcionar inteligencia en análisis de seguridad e inteligencia sobre amenazas a toda la empresa. Con Microsoft Sentinel obtendrá una única solución para la detección de ataques, la visibilidad de amenazas, la búsqueda proactiva y la respuesta contra amenazas.
3. Microsoft Sentinel permite obtener una vista general de toda la empresa, lo que suaviza la tensión de ataques cada vez más sofisticados, volúmenes de alertas cada vez mayores y plazos de resolución largos.
4. Microsoft Sentinel le permite:
    - Recopilar datos de todos los usuarios, dispositivos, aplicaciones y de toda la infraestructura, tanto en el entorno local como en la nube.
    - Detectar amenazas que antes no se detectaban y minimizar falsos positivos mediante el análisis y la inteligencia sobre amenazas sin precedentes.
    - Investigar amenazas con inteligencia artificial y buscar actividades sospechosas.
    - Responder a los incidentes con rapidez con la orquestación y la automatización de tareas comunes integradas.

2. OBJETO Y ALCANCE

5. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft Sentinel.

6. Este servicio ha sido cualificado, e incluido en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) en la Familia de Sistemas de gestión de eventos de seguridad (SIEM) de la taxonomía definida por el Centro Criptológico Nacional en la guía CCN-STIC 140.

3. ORGANIZACIÓN DEL DOCUMENTO

Este documento se compone de los siguientes apartados:

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del servicio.

b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del servicio.

c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del servicio, para lograr una configuración segura.

d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del servicio.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL SERVICIO

7. Al tratarse de un servicio en la nube, se dará de alta los datos del cliente en la plataforma de **Microsoft Office 365 (REF1)** y se enviarán de forma segura los accesos pertinentes a la plataforma.
8. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
9. Una vez dado el alta en la plataforma se podrá activar las licencias por cada usuario dentro de la plataforma (ver sección **4.3**).

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el servicio.
11. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras.
12. Sólo los usuarios autorizados y con la licencia activa podrá acceder al servicio.

4.3 REGISTRO Y LICENCIAS

13. Los servicios prestados son mediante contratación y no es necesario la instalación.
14. Las licencias se activan por cada usuario dentro de la suscripción contratada.

4.4 CONSIDERACIONES PREVIAS

15. Como corresponde a un servicio en la nube, la principal consideración previa es tener conexión a internet y estar dado de alta en la plataforma para hacer uso del servicio.
16. Los prerrequisitos necesarios para la implementación del servicio están descritos en el enlace de **Requisitos previos para la implementación de Microsoft Sentinel** (**REF2**).

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. El servicio consta de los siguientes componentes:
    - Portal: Permite visualizar los eventos recibidos, administrar e investigar las alertas generadas.
    - Conectores de datos: Conectores de datos se encargan de enviar datos de diferentes fuentes para que después Microsoft Sentinel pueda mostrar los eventos y generar alertas. Estos conectores pueden ser para la conexión de datos externos (Syslog, Common Event Format (CEF) o REST APIs) e internos de Microsoft (Office 365, id. de Microsoft Entra, Microsoft Defender for Identity y Microsoft Defender for Cloud Apps).
    - Log Analytics: Log Analytics es una herramienta de Azure Portal que se usa para editar y ejecutar consultas de registro en los datos del almacén de registros de Azure Monitor.

18. El servicio no requiere de otros componentes externos para cumplir con su funcionalidad de seguridad.

5. FASE DE INSTALACIÓN

19. En este apartado se describe la implementación del servicio. Consta de los siguientes pasos:

    - Alta del servicio en la nube.
    - Despliegue de Microsoft Sentinel.

5.1 ALTA DEL SERVICIO EN LA NUBE

20. Al tratarse de un servicio en la nube, lo único que se requiere para ser utilizado es que el proveedor del servicio asigne un usuario en el sistema.

21. Una vez dado de alta, los usuarios autorizados podrán acceder al portal y proceder a la implementación de los demás componentes.

5.2 DESPLIEGUE DE MICROSOFT SENTINEL

22. Para ver los procesos de despliegue, seguir los pasos de la sección 2 de la guía CCN-STIC 884E Guía de configuración segura para Azure Sentinel (**REF8**).

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

23. Al ser un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el servicio.

24. El acceso se realiza mediante el uso de HTTPS con TLS1.2 o superior para las comunicaciones seguras y sólo los usuarios autorizados podrán acceder al servicio. Todos los usuarios deben ser autenticados por Azure AD antes de cualquier interacción con el servicio.

25. El servicio es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure AD. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del servicio.

26. Respecto al cliente no es necesario ninguna configuración segura ya que todo se realiza desde el portal de Microsoft 365 Defender.

27. Microsoft Sentinel viene con muchos conectores listos para usar para los servicios de Microsoft, que se integran en tiempo real. (Por ejemplo, el conector XDR de Microsoft Defender). Para conectores de datos para servicios que no son de Microsoft, cada conector de datos tiene su manera de comunicarse (Por ejemplo, Syslog, Common Event Format (CEF) o REST APIs).

28. Para más información consulta **Conectores de datos de Microsoft Sentinel (REF9)** y en **Búsqueda del conector de datos de Microsoft Sentinel (REF4)** se pueden visualizar los conectores de datos disponibles y la configuración necesaria para incorporarlos a Microsoft Sentinel.

6.2 AUTENTICACIÓN

29. El servicio usa Azure Active Directory para que los usuarios se autentiquen antes de cualquier interacción con el servicio cuando el acceso se realiza a través de la interfaz web. Para la autenticación de los conectores basados en API se utiliza el id. del área de trabajo y la clave del área de trabajo (clave principal) del servicio. Para los conectores externos se basa en despliegues de agentes que reenvían los datos mediante el uno de TLS.

30. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC). Un rol concede los permisos para realizar un conjunto de tareas y un grupo de roles es un conjunto de roles que permite a los usuarios realizar las tareas en el servicio. Un usuario puede ser miembro de un rol. El servicio puede usar varios roles.

31. Azure Multi-Factor Authentication (MFA) protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación.

32. Más información en la guía CCN-STIC-884A Guía de configuración segura para Azure (**REF8**).

6.3 ADMINISTRACIÓN DEL SERVICIO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

33. Como el servicio forma parte de la infraestructura de Microsoft Azure, la administración se realiza de forma remota utilizando el protocolo seguro HTTPS con TLSv1.2 o superior para el establecimiento de las comunicaciones seguras.
34. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

35. Al formar parte el servicio de la infraestructura de Microsoft Azure, la administración se realiza de forma remota.
36. El servicio es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure AD. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del servicio.
37. Algunos de estos roles y funciones pueden ser los siguientes:
    - Global administrator: Puede administrar todos los aspectos del identificador de Azure AD y los servicios de Microsoft que usan identidades de Azure AD.
    - Security administrator: Puede leer información e informes de seguridad, y administrar la configuración en Azure AD y Office 365.
    - Global reader: Puede leer todo lo que puede leer un administrador global, pero no actualizar nada.
38. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Microsoft Entra built-in roles (REF6).**
39. El servicioforma parte de la infraestructura de Azure y usa Azure AD para administrar las cuentas de usuario. Las sesiones expiran después de un período establecido por el administrador en Azure AD. Los valores predeterminados son:
    - Duración máxima de la sesión: 1440 minutos.
    - Duración mínima de la sesión: 60 minutos.
    - Cuánto tiempo antes de que expire la sesión antes de que se muestre la advertencia de tiempo de espera: 20 minutos.
40. El servicio utiliza Azure AD para las cuentas, y se aplican diferentes mecanismos de seguridad como la tecnología Smart Lockout. El bloqueo inteligente protege las cuentas de usuario de los ataques que intentan adivinar las contraseñas de los usuarios o utilizan métodos de fuerza bruta para entrar. Los valores predeterminados de bloqueo inteligente son los siguientes:
    - Umbral de bloqueo (número de intentos de inicio de sesión fallidos antes de que se bloquee a un usuario): 10.
    - Duración del bloqueo: 60 segundos.

41. El servicio utiliza la infraestructura de Azure y puede administrar la directiva de contraseñas mediante las directivas de Azure AD. Se aplica una directiva de contraseñas a todas las cuentas de usuario y administrador que se crean y administran directamente en Azure AD. Los siguientes requisitos de directiva de contraseñas de Azure AD se aplican a todas las contraseñas que se crean, cambian o restablecen en Azure AD:

Propiedad	Requisitos
Caracteres permitidos	Mayúsculas (A - Z) Minúsculas (a - z) Números (0 - 9) Símbolos: - @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > Espacio en blanco
Caracteres no permitidos	Caracteres unicode
Longitud de la contraseña	Un mínimo de 8 caracteres y un máximo de 256.
Complejidad de contraseñas	Las contraseñas requieren 3 categorías de las 4 siguientes: - Mayúsculas - Minúsculas - Números - Símbolos
Contraseña no utilizada recientemente	Cuando un usuario cambia o restablece su contraseña, la nueva contraseña no puede ser la misma que las contraseñas actuales o usadas recientemente.

Tabla 1: Política de contraseñas

42. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Documentación de autenticación de Microsoft Entra (REF7).**

43. En la sección 3.1.1 de la guía CCN-STIC 884E Guía de configuración segura para Azure Sentinel (**REF8**) está definido el control de acceso implementado por el servicio.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

44. Todo acceso al servicio se realiza mediante el uso de HTTPS con TLS1.2 o superior.

45. Los conectores se comunican con el servicio mediante el uso de HTTPS con TLS1.2 o superior. Ver Conectores de datos de Microsoft Sentinel (**REF9**).

6.5 GESTIÓN DE CERTIFICADOS

46. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure y los certificados usan RSA con longitud de clave de 2048 bits.

6.6 SERVIDORES DE AUTENTICACIÓN

47. El servicio usa Azure Active Directory para que los usuarios se autentiquen antes de cualquier interacción con el servicio cuando el acceso se realiza a través de la interfaz web. Ver sección 2 y 3 de la guía CCN-STIC 884E Guía de configuración segura para Azure Sentinel (**REF8**).

6.7 SINCRONIZACIÓN

48. Al tratarse de un servicio en la nube, los servidores donde está alojado el servicio se sincronizan mediante el uso de NTP con el proveedor de servicios en la nube.

6.8 ACTUALIZACIONES

49. El proveedor de servicios en la nube actualiza el software en sus servicios administrados, y se encarga de mantener sus sistemas actualizados sin la intervención del usuario.

6.9 ALTA DISPONIBILIDAD

50. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube brinda el servicio de alta disponibilidad sobre los servidores donde se aloja el servicio y las conexiones para el acceso al mismo.

6.10 AUDITORÍA

6.10.1 REGISTRO DE EVENTOS

51. El servicio genera registros de auditoría clasificados por actividades que se auditan en Microsoft 365. Puede buscar estos eventos buscando en el registro de auditoría en el portal de seguridad y cumplimiento seleccionando la categoría:

    - Proceso de inicio de sesión del personal autorizado (estos eventos son de la integración con Azure AD). Debido a la arquitectura y el modo de funcionamiento de la infraestructura de Azure, la plataforma usa la funcionalidad de sesiones y no hay eventos de cierre de sesión. Los inicios de sesión (sing-ins) se registran con los siguientes estados descritos:
        - Éxito: inicio de sesión exitoso.
        - Error: Error al validar las credenciales debido a un nombre de usuario o contraseña no válidos.

- Interrumpido: la contraseña del usuario ha caducado y, por lo tanto, su inicio de sesión o sesión ha finalizado. Donde se le pregunta a un usuario si desea permanecer conectado a este navegador para facilitar los inicios de sesión posteriores.

- Cambio en las credenciales de usuario (estos eventos son de la integración con Azure AD)
- Eventos relacionados con los roles: Creación, borrado de asignación de rol.
- Eventos relacionados con la funcionalidad:
  - Reglas de alertas: Alerta sobre la creación y actualización del log de actividad.
  - Habilitar/deshabilitar características (Tabla de anomalías)

52. Los eventos de auditoria se consultan en la página de Azure Activity Log. Estos eventos contienen la siguiente información:
    - Nombre de la operación: Breve descripción de la operación llevada a cabo (tipo de evento).
    - Estado: resultado del evento (salida).
    - Marca de tiempo: fecha del evento (fecha/hora del evento).
    - Subscripción: Nombre de la subscripción afectada.
    - Evento iniciado por: Entidad que ha iniciado el evento (sujeto).

53. Microsoft Sentinel proporciona acceso a:
    - La tabla **AzureActivity**, en la que se proporcionan detalles sobre todas las acciones realizadas en Microsoft Sentinel, como la edición de reglas de alertas.
    - La tabla **LAQueryLogs**, en la que se proporcionan detalles sobre las consultas que se ejecutan en log Analytics, incluidas las consultas que se ejecutan desde Microsoft Sentinel.

54. Para más información consultar **Auditoría de consultas y actividades de Microsoft Sentinel (REF10).**

6.10.2 ALMACENAMIENTO LOCAL

55. Al tratarse de un servicio en la nube, el almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada. El almacenamiento en reposo de la información se lleva a cabo mediante el uso de la infraestructura de Azure empleando el cifrado con AES-256 bits.

6.10.3 ALMACENAMIENTO REMOTO

56. La opción de enviar eventos de registros a un servidor no está disponible. Solo se pueden enviar los registros a una cuenta de Azure Storage o a Azure Event Hubs.

57. En el caso de Azure Event Hubs, se realizará la configuración desde la funcionalidad de Azure Monitor Log. Ver Transmisión de datos de supervisión de Azre a un centro de eventos o asociado externo (**REF12**).

6.11 BACKUP

58. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft Azure.

59. Se pueden consultar las opciones de backup en la sección 3.2.2.3 de la guía CCN-STIC 884E Guía de configuración segura para Azure Sentinel (**REF8**).

6.12 FUNCIONES DE SEGURIDAD

60. Este apartado se debe consultar en la CCN-STIC-884E Guía de Configuración segura para Azure Sentinel (**REF8**).

7. FASE DE OPERACIÓN

61. Al tratarse de un servicio en la nube, las consideraciones para realizar una operación segura del mismo deben ser tenidas en cuenta por el proveedor del servicio.

62. No obstante, el cliente deberá tener en cuenta las siguientes tareas para una operación segura del servicio:

    - Analizar periódicamente los registros de auditoría generados por el servicio con el objetivo de detectar cualquier comportamiento anómalo del mismo.
    - Los administradores deben estar correctamente formados en el uso y la correcta operación del servicio.
    - Los administradores mantendrán sus credenciales de acceso al servicio seguras y protegidas.
    - Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.
    - **Revisión de contenido de soluciones o contenido independiente.** Obtenga las actualizaciones de contenido de las soluciones instaladas o contenido independiente del Centro de contenido.
    - **Revisar el acceso de usuario.** Revise los permisos de los usuarios y compruebe si hay usuarios inactivos.
    - **Conectores de datos.** Revise el estado, la fecha y la hora del último registro recibido de cada conector de datos para asegurarse de que los datos fluyen. Compruebe si hay nuevos conectores y revise la ingesta de datos para asegurarse de que no se han superado los límites establecidos.
    - **Log Analytics.** Compruebe que los servidores y estaciones de trabajo están conectados activamente al área de trabajo y corrija las conexiones fallidas.
    - Para más información consultar **Procedimientos recomendados de Microsoft Sentinel (REF11).**

8. REFERENCIAS

REF1 Microsoft Office 365
https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing

REF2 Requisitos previos para implementar Microsoft Sentinel
Requisitos previos para la implementación de Microsoft Sentinel | Microsoft Learn

REF3 Creación de un área de trabajo de Log Analytics
https://learn.microsoft.com/es-es/azure/azure-monitor/logs/quick-create-workspace

REF4 Búsqueda del conector de datos de Microsoft Sentinel
https://learn.microsoft.com/es-es/azure/sentinel/data-connectors-reference

REF5 Inicio rápido: Incorporación a Microsoft Sentinel
https://learn.microsoft.com/es-es/azure/sentinel/quickstart-onboard

REF6 Microsoft Entra built-in roles
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

REF7 Documentación de autenticación de Microsoft Entra
https://learn.microsoft.com/es-es/entra/identity/authentication/

REF8 CCN-STIC 884E Guía de configuración segura para Azure Sentinel
https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/6299-ccn-stic-884e-guia-de-configuracion-segura-para-azure-sentinel/file.html

REF9 Conectores de datos de Microsoft Sentinel
https://learn.microsoft.com/es-es/azure/sentinel/connect-data-sources

REF10 Auditoría de consultas y actividades de Microsoft Sentinel
https://learn.microsoft.com/es-es/azure/sentinel/audit-sentinel-data

REF11 Procedimientos recomendados de Microsoft Sentinel
https://learn.microsoft.com/es-es/azure/sentinel/best-practices

REF12 Transmisión de datos de supervisión de Azre a un centro de eventos o asociado externo.
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/stream-monitoring-data-event-hubs

9. ABREVIATURAS

AD	Directorio Activo
AES	Advanced Encryption Standard
CCN	Centro Criptográfico Nacional
CEF	Formato de Eventos Comunes
CLI	Interfaz de Línea de Comandos
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
ENS	Esquema Nacional de Seguridad.
HTTP	Hyper Text Transfer Protocol
NTP	Network Time Protocol
RBAC	Control de Acceso Basado en Roles
SIEM	Administración de Eventos e Información de Seguridad
SOAR	Respuesta Automatizada de Orquestación de Seguridad
TLS	Transport Layer Security
SIEM	Security Information and Event Management

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL