

OTRAS DISPOSICIONES

DEPARTAMENTO DE SEGURIDAD

2916

RESOLUCIÓN de 10 de junio de 2022, del Director de Juego y Espectáculos, por la que se establecen las especificaciones técnicas que deben cumplir los sistemas de control de admisión de los locales de juego para la conexión con el registro de interdicciones de acceso al juego.

El Decreto 19/2022, de 8 de febrero, por el que se modifica el Decreto 120/2016 por el que se aprueba el reglamento general del juego en la Comunidad Autónoma de Euskadi, establece la obligatoriedad de un sistema de control de admisión situado en la entrada de los locales de juego, que impida el acceso a aquellas personas que lo tengan prohibido conforme al artículo 17.

El apartado 2 de dicho artículo establece que, para ello, «el control de admisión deberá disponer de un sistema informático que permita la conexión con el registro de interdicciones de acceso al juego, según especificaciones establecidas por resolución de la persona titular de la Autoridad Reguladora del Juego».

A la vista de todo lo expuesto, y en virtud de las competencias atribuidas por el artículo 20 del Decreto 19/2022, de 8 de febrero, por el que se modifica el Decreto 120/2016 por el que se aprueba el reglamento general del juego en la Comunidad Autónoma de Euskadi, y por las atribuciones que me son conferidas por el Decreto 6/2021, de 19 de enero, por el que se establece la estructura orgánica y funcional del Departamento de Seguridad.

DISPONGO:

Primero.– Establecer las especificaciones técnicas mínimas que deben cumplir los sistemas de control de admisión de los locales de juego para la conexión con el registro de interdicciones de acceso al juego en los términos recogidos en el anexo.

Segundo.– Notifíquese esta resolución a la Unidad de Juego y Espectáculos de la Ertzaintza.

Tercero.– Esta Resolución se publicará en el Boletín Oficial del País Vasco.

DISPOSICIÓN FINAL

Contra la presente Resolución, que no agota la vía administrativa, podrá interponer ante el Viceconsejero de Seguridad, el correspondiente recurso de alzada, en el plazo de UN MES a partir del día siguiente a su publicación, según lo establecido en los artículos 121 y siguientes de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En Vitoria-Gasteiz, a 10 de junio de 2022.

El Director de Juego y Espectáculos,
AITOR MIKEL URIARTE UNZALU.

ANEXO

ESPECIFICACIONES TÉCNICAS QUE DEBEN CUMPLIR LOS SISTEMAS DE CONTROL DE ADMISIÓN DE LOS LOCALES DE JUEGO PARA LA CONEXIÓN CON EL REGISTRO DE INTERDICCIÓN DE ACCESO AL JUEGO

1.– Web service.

El fabricante inscrito en el registro General de Juego deberá de desarrollar un servicio Web-Service (WS) sobre protocolo SOAP con una capa adicional de seguridad, por la cual los parámetros que se envíen han de estar cifrados mediante el algoritmo AES/ECB y una clave de 128 bits. Igualmente, la respuesta obtenida será devuelta cifrada bajo la misma clave.

El WS a desarrollar realizará un XML de consulta y recibirá un XML de respuesta.

2.– URL.

La Dirección de Juego y Espectáculos (DJE) aportará, en el propio procedimiento telemático de homologación de sistemas o aplicaciones que deban controlar el acceso, la URL a través de la cual se realizará la consulta al registro de interdicciones de acceso al juego.

3.– XML's de consulta y respuesta.

El servicio dispondrá de una operación de nombre procesarLlamadaEncrypt que recibirá como parámetro un xml de consulta, el cual se enviará cifrado con una clave de 128 bits que habrá sido previamente facilitada por el departamento.

El xml de consulta tiene la siguiente estructura:

- Usuario: Usuario que intenta acceder al servicio Web (proporcionado por la DJE).
- Password: contraseña del usuario que intenta acceder al servicio Web (que también ha de estar codificado previamente en base64) (proporcionado por DJE).
- Método: puede tomar 2 valores
 - o Método validarRegistro el cual deberá utilizarse en el momento que un usuario se registra en la aplicación del fabricante, donde se comprueba que el usuario sea mayor de edad y que no esté inscrito en el registro de prohibidos de la Dirección de Juegos y Espectáculos.
 - o Método validarAcceso el cual deberá utilizarse en el momento que un usuario realiza el login a la aplicación del fabricante, donde se comprueba que el usuario no esté inscrito en el registro de prohibidos de la Dirección de Juegos y Espectáculos.
- Documento de identidad (DNI, NIE, tarjeta de residencia o pasaporte) de la persona respecto a la que el servicio Web nos debe indicar si tiene acceso o no lo tiene.
- Tipo Documento: tipo documento de identificación DNI, NIE, tarjeta de residencia, pasaporte.
- Fecha nacimiento: Fecha de nacimiento con formato AAAAMMDD. Obligatorio para el método de validarRegistro.

Tipos de errores producidos, se devuelven dentro del SoapFault y se especifican en el protocolo realizado para el desarrollo del WS y que está disponible en la página web de la DJE.

Un elemento SOAP Fault contiene información del error que se ha producido. Contiene los siguientes elementos:

- faultCode: obligatorio. Valores que puede tomar:
 - Client: el SOAPMessage no es correcto o no contiene información suficiente. El error está provocado por lo que manda el cliente.
 - Server: el SOAPMessage no se ha procesado correctamente por un error de procesamiento en el servidor.
 - VersionMismatch: el namespace del SOAPEnvelope no es válido.
 - MustUnderstand: un elemento de un SOAPHeader tiene el atributo mustUnderstand a true, pero el servidor no lo reconoce.
- faultString: obligatorio. Texto explicativo del error.
- faultActor: opcional. Actor que ha causado el error. En nuestros servicios web no estamos definiendo actores. En la invocación de los servicios web de integración son irrelevantes.
- elemento Detail: opcional. Contiene los detalles del error.

El XML de respuesta, ante la consulta de un documento de identidad, devolverá «S» si está prohibido o «N» si no lo está.

4.– Incidencias.

El operador del local deberá tratar todos los mensajes de error que devuelva el sistema y deberá recoger de forma manual los datos de la persona que accede al local (documento de identificación), fecha y hora, a efectos del control e inspección. Todo ello conforme al Reglamento General de Protección de Datos y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

5.– Otras especificaciones.

- La empresa que instale el sistema o aplicación, deberá, en todas las ocasiones, hacer la comprobación de que la persona que quiera acceder al local o a la aplicación, no figura en el fichero del Registro de Interdicciones de acceso al juego de Euskadi y que no es menor de edad.
- El personal del local y el sistema de forma automática en sucesivas visitas, verificarán fehacientemente la identidad de la persona que pretende acceder y confirmar que realmente es esa persona; ya que, si solo se verifica la documentación, se podría acceder con un documento que no corresponde con el de la persona que accede.
- La Unidad de Juego de la Ertzaintza (UJE) para poder comprobar «in situ» si una persona ha pasado por el control establecido, debe poder consultar el DNI, pasaporte u otros medios admitidos en derecho y la hora de paso por el control en la aplicación o sistema a instalar.
- La empresa podrá guardar datos de registro e identificativos de las personas que acceden, siempre que lo hagan bajo su responsabilidad y con sus correspondientes declaraciones de ficheros de carácter personal, conforme al Reglamento General de Protección de Datos y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. La pertenencia a este fichero no exime de su comprobación previa y obligatoria a través del Webservice establecido.

- Con fines estadísticos, el sistema deberá monitorizar y a petición de la Autoridad reguladora del juego deberá remitir la siguiente información:
 - Flujo de entrada.
 - Resultado de la consulta (válido o no válido).
 - Fecha y hora de la consulta.
- Los sistemas a establecer en los locales de juego, basados en barreras, tornos o sistemas similares, tienen que ser desbloqueados, ya sea manual o automáticamente, ante una emergencia de desalojo, priorizando el desbloqueo automático conectado al sistema de alarma en los casos en que el local disponga de la misma. Aun y cuando el sistema sea automático y esté conectado a la alarma, será obligatorio la posibilidad de accionamiento manual del control de acceso para los casos en los que el hecho causante no active la alarma. En todo momento deberá haber una persona instruida y encargada del accionamiento manual de desbloqueo.
- Los elementos instalados no deben ser susceptibles de dificultar el paso ante una situación de emergencia. no pudiendo reducir la anchura de las vías de evacuación, ya que con esto se disminuye la capacidad de evacuación del local.
- Los elementos instalados deben de cumplir con lo indicado en las Normas Técnicas del Decreto 68/2000 sobre condiciones de accesibilidad del Gobierno Vasco y las Exigencias Básicas de Seguridad de Utilización y Accesibilidad del CTE-DB SUA.
- Todo ello sin perjuicio de la normativa específica aplicable a los locales de concurrencia pública y de juego.