

# Sistema de Gestión de la Ciberseguridad

Requisitos de ciberseguridad para proveedores



# Requisitos de ciberseguridad para proveedores

Versión	Fecha	Descripción
1.0	25/05/2022	Versión Inicial
1.1	15/04/2024	Revisión del documento
1.2	25/04/2024	Revisión del documento

## CLASIFICACIÓN DEL DOCUMENTO

USO OFICIAL-INTERNO
<p><b>Nota de confidencialidad:</b> la información contenida en el presente documento ha sido calificada como USO OFICIAL-INTERNO y solo puede ser utilizada de acuerdo con las cláusulas establecidas por Metro de Madrid, S.A.</p> <p>Es responsabilidad del personal receptor/a de este documento su distribución en base a la necesidad del contenido del mismo.</p>

## INDICE DE CONTENIDO

1.	Documentación de referencia .....	4
2.	Objeto.....	4
3.	Alcance .....	4
4.	Requisitos generales.....	4
4.1	Marco legal, regulatorio y normativo en materia de ciberseguridad .....	4
4.2	Marco de referencia para la gestión de la ciberseguridad.....	5
4.3	Arquitectura de seguridad .....	5
4.4	Seguridad en el ciclo de vida de los sistemas de información .....	6
4.5	Seguridad en la cadena de suministro .....	6
4.6	Incidentes de ciberseguridad .....	6
4.7	Ubicación y tratamiento de la información .....	7
4.8	Cumplimiento de la normativa vigente de protección de datos .....	7
4.9	Propiedad intelectual .....	7
4.10	Finalización del contrato.....	8
4.11	Cláusula de confidencialidad .....	8
5.	Requisitos específicos.....	8
5.1	Control de acceso lógico: .....	8
5.1.1	Control de Acceso a Redes y Servicios de Red .....	9
5.1.2	Control de Acceso a Sistemas Operativos, Bases de Datos y Aplicaciones .....	9
5.2	Registros de actividad:.....	10
5.3	Gestión de la configuración.....	11
5.4	Claves criptográficas .....	11
5.5	Configuración de seguridad.....	11
5.6	Seguridad de las comunicaciones .....	12
5.7	Redes inalámbricas.....	13
5.8	Control del software malicioso.....	14
5.9	Desarrollo de software .....	14
5.10	Gestión de vulnerabilidades.....	15

5.11	Aceptación del sistema .....	15
6.	Cualificaciones profesionales de Seguridad de la Información .....	16
7.	Mecanismos de coordinación en ciberseguridad.....	16

## 1. Documentación de referencia

- UNE-EN ISO/IEC 27001:2017 Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información– Requisitos.
- UNE-EN ISO/IEC 27002:2017 Tecnología de la Información – Técnicas de Seguridad – Código de Prácticas para los Controles de Seguridad de la Información.
- UNE-EN IEC 62443-3-3:2020 Redes de comunicaciones industriales Seguridad de la red y del sistema – Parte 3-3: Requisitos de seguridad del sistema y niveles de seguridad.
- UNE-CLC/TS 50701:2021: Aplicaciones ferroviarias. Ciberseguridad.
- Abstract - Obligaciones de los prestadores de servicios a las entidades públicas: Documento publicado por el CCN-CERT.
- Guía sobre controles de seguridad en sistemas OT publicada por la Secretaría de Estado de Seguridad – Ministerio del Interior – Gobierno de España.
- Guía CCN-STIC 823 – Utilización de servicios en la nube

## 2. Objeto

El objeto del presente documento es establecer los requisitos mínimos en materia de ciberseguridad que deberán cumplir los proveedores de Metro de Madrid S.A. (en lo sucesivo, Metro de Madrid).

## 3. Alcance

El presente documento aplica a:

- Proveedores de tecnologías de la información, tecnologías de la operación y de comunicaciones que presten servicios para Metro de Madrid.
- Sistemas de información de Metro de Madrid. Esto incluye, entre otros:
  - Tecnologías de la Información (IT).
  - Tecnologías de la Operación (OT).
  - Sistemas de Comunicación y telecomunicaciones.
  - Los datos y la información propiedad de Metro de Madrid.

## 4. Requisitos generales

### 4.1 Marco legal, regulatorio y normativo en materia de ciberseguridad

Para la realización de los trabajos objeto del contrato, deben tenerse en cuenta, al menos, las siguientes referencias:

- **En cuanto al marco legal, regulatorio y normativo:**
  - Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (Directiva NIS).

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- **En cuanto a códigos de buenas prácticas y otras normativas específicas:**

- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información.
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.
- Guías CCN-STIC.

Se considerarán todas las modificaciones y ampliaciones de las citadas normas.

## 4.2 Marco de referencia para la gestión de la ciberseguridad

El adjudicatario:

- Deberá cumplir con las directrices establecidas en la Política de Ciberseguridad de Metro de Madrid y en el cuerpo documental (normas y procedimientos) que deriven de la misma.
- Deberá disponer de una metodología formal de gestión de la ciberseguridad (políticas, normas, procedimientos, etc.) la cual deberá ser aplicada durante todas las fases del ciclo de vida de los productos y/o servicios objeto del contrato.
- Abordará la gestión de la ciberseguridad desde un enfoque basado en el riesgo.
- Identificará claramente los controles de ciberseguridad (físicos, lógicos, procedimentales, entre otros) que aplicará al producto/servicio.
- Verificará y demostrará, según sea necesario, que la implementación de los mismos no afecte desfavorablemente a la conectividad, la latencia, el ancho de banda, el tiempo de respuesta y al rendimiento.

## 4.3 Arquitectura de seguridad

El adjudicatario deberá aportar la información necesaria sobre el sistema que soporta los servicios respecto a la arquitectura de seguridad, con el objeto de facilitar a Metro de Madrid el cumplimiento de sus obligaciones, tales como la realización del Análisis de Riesgos de Ciberseguridad o el subsiguiente Plan de Tratamiento de Riesgos.

Asimismo, aportará los diagramas de red, esquemas de elementos físicos, esquemas de interconexión y esquemas lógicos de sistemas que detallen la infraestructura física y lógica de la que forma parte el producto / servicio objeto de contratación.

De esta forma, Metro de Madrid validará la arquitectura de ciberseguridad y podrá delimitar las dependencias entre los diferentes activos y analizar las potenciales amenazas que se podrían materializar sobre los sistemas de información.

#### **4.4 Seguridad en el ciclo de vida de los sistemas de información**

El adjudicatario deberá integrar los requisitos de ciberseguridad establecidos en el presente documento, en las distintas fases del ciclo de vida de los productos y/o servicios objeto del contrato.

Asimismo, durante la fase de diseño, el adjudicatario deberá realizar una caracterización de amenazas; esto es, la definición de las principales áreas/puntos donde el sistema de información -instalaciones, sistemas, comunicaciones, aplicaciones o cualquier otro punto susceptible de ser atacado- es vulnerable. Una vez identificadas estas áreas, se deberán seleccionar las medidas más adecuadas para mitigar las amenazas detectadas.

#### **4.5 Seguridad en la cadena de suministro**

El adjudicatario deberá:

- Disponer de una documentación que detalle claramente los elementos que forman parte de la cadena de subcontratación, así como las implicaciones derivadas de cualquier cambio o modificación que pueda sufrir algún eslabón de dicha cadena.
- Asegurar que los sistemas de información de las empresas subcontratadas cumplen con los requisitos de ciberseguridad establecidos en el presente documento.
- Garantizar que los riesgos de terceras partes son controlados mediante el establecimiento de una metodología de gestión de la ciberseguridad.
- Garantizar que los controles de la cadena de suministro protejan los sistemas de información durante todas las fases del ciclo de vida de los mismos (diseño, despliegue, transporte, explotación, mantenimiento y desmantelamiento).

#### **4.6 Incidentes de ciberseguridad**

Metro de Madrid tiene la obligación de notificar los incidentes de ciberseguridad que le afecten.

En este sentido, el adjudicatario deberá notificar al Responsable de Seguridad de la Información de Metro de Madrid, a la mayor brevedad posible, los incidentes de ciberseguridad que puedan afectar la seguridad de los sistemas objeto del servicio o de la plataforma tecnológica de Metro de Madrid.

Para ello, el adjudicatario definirá un procedimiento para la detección, notificación y tratamiento de incidentes de ciberseguridad. Todo el personal involucrado en los trabajos deberá ser formado en estos procedimientos.

A su vez, el adjudicatario deberá colaborar con Metro de Madrid en la resolución de incidentes de seguridad que afecten a los productos y/o servicios objeto del contrato, a fin de calibrar el impacto del incidente y definir las medidas necesarias de contención, mitigación, respuesta y recuperación.

#### **4.7 Ubicación y tratamiento de la información**

Los datos e información propiedad de Metro de Madrid (documentos, ficheros, planos, datos almacenados en sistemas, etc.) serán tratados de acuerdo a su nivel de confidencialidad y según lo establecido en los procedimientos de clasificación y tratamiento de la información de Metro de Madrid.

Por otro lado, en aquellos casos en los que los datos se alojen en sistemas del prestador del servicio, o de terceras partes subcontratadas por este, el adjudicatario deberá:

- Informar a Metro de Madrid sobre la ubicación geográfica de los datos (incluido copias de seguridad (backups) y almacenamiento de logs), antes y durante el suministro del servicio.
- Indicar las medidas de seguridad física asociadas a las instalaciones desde las que se prestan los servicios.

#### **4.8 Cumplimiento de la normativa vigente de protección de datos**

En aquellos casos en los que los servicios prestados impliquen el tratamiento de datos personales, será necesario la implementación de funcionalidades que garanticen el cumplimiento de la normativa vigente por parte de la entidad pública cliente. Por ejemplo, medidas destinadas a cumplir con los principios básicos del tratamiento y que permitan garantizar los derechos de los interesados (acceso, rectificación, supresión, bloqueo de datos, etc.).

Además de lo anterior, cuando resulte procedente, el proveedor de servicios estará obligado a cumplir las obligaciones que establece la normativa de protección de datos para los Encargados de Tratamiento.

#### **4.9 Propiedad intelectual**

Los desarrollos a medida realizados por el adjudicatario en el marco del contrato serán propiedad de Metro de Madrid.

La titularidad del desarrollo afecta no sólo al producto final, sino al conjunto de trabajos, bocetos, esquemas, documentos previos, diagramas de flujo y, en conjunto, todos y cada uno de los trabajos susceptibles de ser objeto de propiedad intelectual e industrial realizados para el desarrollo.



## 4.10 Finalización del contrato

El adjudicatario deberá definir e implementar mecanismos que garanticen la portabilidad de la información con el objetivo de facilitar a Metro de Madrid el proceso de gestión del cambio ante el cese o baja de los servicios suministrados por parte del mismo.

Asimismo, el adjudicatario deberá certificar que, al causar baja el servicio suministrado, los datos almacenados en sus sistemas, o en sistemas de terceras partes subcontratadas, han sido eliminados de manera segura una vez finalizado el proceso de portabilidad.

## 4.11 Cláusula de confidencialidad

El Adjudicatario:

- Firmará un acuerdo de confidencialidad en el que se comprometa a no revelar información de Metro de Madrid, tanto durante la duración del contrato como después de la finalización del mismo.
- Establecerá los mecanismos de control necesarios para asegurar que sus empleados y terceras partes contratadas por este, cumplen con lo establecido en el acuerdo de confidencialidad.
- No deberá publicar en su página web ni en cualquier otro foro público o privado, información que haga referencia a Metro de Madrid (productos / servicios implementados; proyectos realizados, etc.), salvo que, previamente, se cuente con la autorización expresa del Responsable de Seguridad de la Información de Metro de Madrid.

## 5. Requisitos específicos

Actualmente, Metro de Madrid está llevando a cabo un proceso de adecuación y certificación de los sistemas de información en el Esquema Nacional de Seguridad (en adelante, ENS), categoría Media.

En este sentido, el adjudicatario deberá aplicar los controles de ciberseguridad que sean necesarios para cumplir con los requisitos establecidos en el ENS Categoría Media. Así mismo, se tendrán en cuenta las guías CCN-STIC que sean de aplicación.

Sin perjuicio de lo anterior, el adjudicatario deberá cumplir las directrices indicadas en los siguientes apartados, en aquellos casos que sean de aplicación.

### 5.1 Control de acceso lógico:

Se deben aplicar controles de acceso en todos los niveles de la arquitectura y topología de los Sistemas de Información. Esto incluye, al menos:

- Redes y servicios de red;
- Plataformas o sistemas operativos;

- Bases de datos;
- Aplicaciones.

### **5.1.1 Control de Acceso a Redes y Servicios de Red**

- El acceso a la red deberá estar controlado por mecanismos de autenticación y autorización que serán de aplicación tanto para equipos como para usuarios y aplicaciones.
- Se deberá garantizar que los equipos, usuarios y aplicaciones no pueden acceder a segmentos de la red donde no tienen permiso para realizar ninguna operación. No se permitirá el acceso a un segmento de red o elemento de red hasta que exista una aprobación expresa a tales efectos.
- Todos los equipos conectados a la red de Metro de Madrid deben ser identificados mediante la MAC de la tarjeta de red, certificado digital u otros medios de identificación segura que garanticen la identificación unívoca de los mismos.
- El adjudicatario no deberá conectar equipos de su propiedad a la red de Metro de Madrid, salvo casos excepcionales en los que se cuente con la autorización expresa del Responsable de Seguridad de la Información de Metro de Madrid.
- Se emplearán elementos de seguridad de red, o sus medidas compensatorias correspondientes, para garantizar o auditar las conexiones de los usuarios, tanto desde redes internas como desde redes externas.
- Los puertos de diagnóstico de los sistemas de Metro de Madrid deben permanecer controlados y protegidos frente accesos no autorizados tanto a nivel físico como lógico. El acceso y configuración de los puertos lógicos y físicos de los dispositivos y sistemas, deben ser restringidos a los administradores y personal de mantenimiento.

### **5.1.2 Control de Acceso a Sistemas Operativos, Bases de Datos y Aplicaciones**

- El acceso a las aplicaciones y bases de datos deben de ser independientes del acceso al sistema operativo que las contiene.
- Sin perjuicio de otros mecanismos más robustos, todos los sistemas de información de Metro de Madrid deben contar con un sistema de validación de usuarios mediante usuario y contraseña.
- Los permisos deberán asignarse, tanto a los usuarios como a las aplicaciones, en la base de necesidad de uso, y en la base de caso por caso, imperando el principio de prohibición de todo excepto lo estrictamente necesario.
- No se permite el uso de identificadores de grupo o genéricos, salvo cuando sea estrictamente necesario y por razones operacionales. Bajo estas circunstancias, toda excepción deberá estar debidamente justificada y aprobada formalmente por el Responsable de Seguridad de la Información de Metro de Madrid, aplicando los controles de seguridad compensatorios.

- Los sistemas cuyo método de autenticación sea por usuario y contraseña, deben disponer de un mecanismo de gestión de contraseñas configurable que permita definir, entre otros:
  - Longitud de la contraseña
  - Periodo de caducidad
  - Número de intentos fallidos
  - Complejidad de la contraseña
- Las aplicaciones publicadas al exterior deben contar con doble factor de autenticación.
- Las contraseñas se almacenarán en bases de datos encriptadas. Asimismo, no se almacenarán contraseñas en ficheros, código de desarrollo o en cualquier tipo de documentación tanto si está en formato impreso como electrónico.
- En aquellos casos en los que los sistemas se alojen en las instalaciones del prestador del servicio, o de terceras partes subcontratadas por este, el adjudicatario establecerá, de forma conjunta con Metro de Madrid, los procedimientos de control de acceso los cuales deberán contemplar al menos:
  - Gestión de solicitudes de alta, baja y modificaciones de usuarios y permisos.
  - Gestión de incidencias relacionadas con el desbloqueo de usuarios y reseteo de contraseñas.
  - Gestión de incidencias relacionadas con los permisos dentro de la aplicación.

## 5.2 Registros de actividad:

- Se deberán implantar mecanismos de registro de actividades (logs) que almacenen los datos generados por las actividades de sistemas, redes, aplicaciones en relación con los administradores, operadores y usuarios base de los sistemas de información. Estos mecanismos de registro deben permanecer activos siempre que dichos sistemas, redes y aplicaciones se encuentren operativos.
- En el caso de que se traten datos de carácter personal sensibles deberá registrarse la siguiente información:
  - Identificación del usuario.
  - Fecha y hora.
  - Fichero accedido.
  - Tipo de acceso.
  - Si el acceso ha sido autorizado o denegado.
  - En caso de accesos autorizados, la información que permita identificar el registro accedido.
- El adjudicatario definirá, de forma conjunta con Metro de Madrid, la información a guardar en los registros de actividad de cada sistema.
- El acceso a las rutas de auditoría y los archivos de registro (logs) estará disponible sólo para usuarios autenticados y autorizados. Además, los archivos de registro (logs) serán inalterables.

- En aquellos casos en los que los sistemas se alojen en las instalaciones del prestador del servicio, o de terceras partes subcontratadas por este, el adjudicatario deberá:
  - Disponer de registros de actividad de los usuarios y sistemas que permitan monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración.
  - Proveer a Metro de Madrid el detalle de los registros de actividad cada vez que sean solicitados.
  - Establecer el procedimiento a seguir para el registro y tratamiento de los logs (Información a registrar, periodicidad de la consolidación y envío de datos a Metro de Madrid, período de retención de los registros, mecanismos implementados para la protección de los registros de actividad, etc.)

### 5.3 Gestión de la configuración

Todo cambio a realizar en los sistemas de Metro de Madrid deberá ser realizado siguiendo los procedimientos de gestión de cambios y gestión de la configuración establecidos por Metro de Madrid.

Asimismo, en aquellos casos en los que los sistemas se alojen fuera de las instalaciones de Metro de Madrid, el adjudicatario deberá definir y comunicar a Metro de Madrid los procedimientos a seguir para la gestión de cambios y gestión de la configuración.

### 5.4 Claves criptográficas

- El adjudicatario implementará sistemas criptográficos para proteger la confidencialidad, integridad, autenticación, autorización y no repudio de los dispositivos y los flujos de datos.
- Tanto el cifrado simétrico como el asimétrico, el intercambio de claves, la autenticación y las validaciones, se harán con robustez suficiente siguiendo la guía CCN-STIC-807 o aquellas que sean de aplicación.
- El adjudicatario deberá proporcionar documentación adecuada que describa los sistemas criptográficos implementados, así como los manuales apropiados para operaciones y mantenimiento.
- En caso de conservar claves criptográficas en la infraestructura del proveedor, este pondrá en conocimiento de Metro de Madrid las medidas implementadas para proteger las mismas durante todo su ciclo de vida (generación, transporte, custodia, retirada y destrucción).

### 5.5 Configuración de seguridad

El adjudicatario deberá:

- Configurar los sistemas de información (servidores, redes, ordenadores y equipos, etc.) tomando como referencia las guías de bastionado publicadas por los fabricantes de los diferentes productos, así como también las disponibles en Metro de Madrid y las publicadas por el CCN-CERT o cualquier otro organismo oficial en materia de ciberseguridad.
- Documentar la configuración asociada a cada sistema, así como también el detalle de guías aplicadas. Entre otros, se deberán especificar los puertos y servicios requeridos para el funcionamiento del sistema.
- Deshabilitar o eliminar cuentas y contraseñas por defecto.
- Aplicar la regla de “mínima funcionalidad”:
  - El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad.
  - Se deben segregar las funciones de administración, operación y auditoría. Asimismo, se definirán perfiles de acceso específicos para cada una de estas funciones, los cuales tendrán los permisos mínimos necesarios.
  - Se debe desactivar mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso aquellas que sean inadecuadas al fin que se persigue.
- Aplicar la regla de “seguridad por defecto”.
- Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo.
- Deshabilitar o eliminar los servicios, componentes de software y herramientas de configuración o diagnóstico instalados en equipos o dispositivos de red cuyo uso no sea necesario para los propósitos de Metro de Madrid.
- Eliminar todos los datos y archivos de configuración no utilizados.
- Proteger la BIOS de cambios no autorizados en la misma, en aquellos equipos que dispongan de dicho elemento. En el caso en que se requiera un cambio de la BIOS, el adjudicatario dispondrá y proporcionará a Metro de Madrid un procedimiento para realizar dicho cambio.

## 5.6 Seguridad de las comunicaciones

- Todos los servicios publicados al exterior de la intranet de Metro de Madrid deben estar publicados en la red frontera de Metro de Madrid (DMZ).

En el caso de sistemas o plataformas que por razones operacionales no puedan cumplir con esta directriz, se seguirán las siguientes premisas:

- Se aplicarán controles de seguridad compensatorios para mitigar el riesgo asociado.
- Se justificará y documentará la excepción.

- La excepción deberá estar aprobada por el Responsable de Seguridad de la Información de Metro de Madrid.
- Todas las aplicaciones web deben ser accesibles únicamente mediante protocolo seguro TLS con versión recomendada en el momento de la implementación por el CCN u otro organismo oficial en materia de ciberseguridad.
- Se deberán emplear protocolos considerados como seguros y soluciones específicas destinadas a tal efecto.
- El acceso a base de datos debe cifrarse en el canal de transporte. Para ello debe habilitarse la opción correspondiente en la cadena de conexión a la base de datos.
- En el lado servidor debe disponerse de certificado SSL expedido por una Autoridad de Certificación confiable.
- La red de Metro de Madrid deberá estar segmentada adecuadamente, a través de dispositivos físicos o lógicos, y de acuerdo a los criterios del negocio y las necesidades para garantizar la Ciberseguridad. Se debe garantizar que exista:
  - Control de entrada de los usuarios que llegan a cada segmento.
  - Control de salida de la información disponible en cada segmento.
- Se ha de garantizar que la herramienta funcione bajo el siguiente entorno de comunicaciones:

**Acceso Interno:**

Balanceador interno F5, se distribuirán las peticiones entre los servidores de las aplicaciones.

- Los flujos de comunicaciones entre todos los elementos del proyecto deben utilizar puertos limitados y definidos.
- Ambos balanceadores hacen el ssl-offload de la conexión https del usuario.
- Debe tener una arquitectura de varias capas, separando los front-ends de herramienta de las bases de datos. Esta separación se realiza mediante firewall corporativos.

**Acceso Externo:**

Balanceador externo F5 que balanceará las peticiones de usuario sobre los frontales o webdispatchers que deben estar ubicados en la DMZ. Los balanceadores cifrarán la conexión extremo a extremo con el usuario de manera que puedan analizar la misma con sus sistemas de seguridad.

## 5.7 Redes inalámbricas

En el caso en que los sistemas de información hagan uso de redes WIFI corporativas, estas deberán contar con las siguientes medidas de seguridad:

- El sistema debe ser capaz de:

- Autenticar en sistemas de autenticación centralizada como servidores RADIUS utilizando canales seguros.
  - Adquirir una IP mediante DHCP para cada cliente / dispositivo en cada una de las distintas redes.
- Configurar los clientes para utilizar los protocolos seguros estándar recomendados por los organismos oficiales en el momento de la implantación y soportados por la infraestructura existente en Metro de Madrid.

## 5.8 Control del software malicioso

El adjudicatario implementará en los equipos las medidas técnicas y procedimentales que sean necesarias para prevenir la infección por software malicioso (malware) y evitar su propagación en caso de infección.

En cuanto a las medidas técnicas, los sistemas deberán contar con capacidades antivirus. En aquellos casos en los que esto no sea posible, el adjudicatario implementará los controles compensatorios que sean necesarios para proteger los sistemas contra el software malicioso.

## 5.9 Desarrollo de software

- El Adjudicatario deberá implementar una metodología de desarrollo seguro durante todo el ciclo de vida del desarrollo del software. Asimismo, informará a Metro de Madrid cuál es la metodología utilizada. En el caso de que no se trate de una metodología estándar del mercado, se indicará de forma detallada las características principales de la misma.
- Toda la actividad de desarrollo de aplicaciones, se realizará en un entorno aislado y en un sistema diferente al de producción.
- En los entornos de producción se prohibirá la existencia de herramientas o de datos pertenecientes a los entornos de desarrollo y, en general, todo software que no sea necesario para la ejecución de sus aplicaciones productivas.
- Se permitirá la inspección del código fuente tanto durante el desarrollo como durante la vida útil del software.
- El adjudicatario deberá demostrar que los sistemas a implementar en el marco del contrato están libres de malware, vulnerabilidades o debilidades resultantes de procesos inseguros de desarrollo y/o pruebas.
- El adjudicatario entregará a Metro de Madrid el código fuente de los desarrollos realizados éste, así como también la documentación de diseño que se considere necesaria para facilitar futuras modificaciones del software.

- Si se utiliza un lenguaje que no sea compilado, deberá asegurarse la limpieza del código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
- Respecto al diseño de los aplicativos o sistemas, se contemplará que, al menos:
  - Dispongan de mecanismos de identificación y autenticación de usuarios, diferenciando los privilegios en cada uno de los entornos existentes, de producción y de desarrollo.
  - Dispongan de mecanismos de protección de la información tratada, conforme al nivel de seguridad de la misma.
  - Dispongan de generación y tratamiento de logs para auditorías.
- El adjudicatario deberá realizar pruebas del software desarrollado las cuales considerarán, entre otros, inspecciones de seguridad de servicio o código:
  - Fugas de información.
  - Puertas traseras de acceso.
  - Escalado de privilegios.
  - Pruebas de desbordamiento de registros.

## 5.10 Gestión de vulnerabilidades

Durante todo el ciclo de vida del contrato y el periodo de garantía, el adjudicatario deberá:

- Notificar cualquier defecto que afecte la ciberseguridad de los Sistemas de la Información de Metro de Madrid tan pronto como éste tenga conocimiento de tal fallo. La notificación incluirá, aunque no está limitada a: documentación detallada de la vulnerabilidad, su causa raíz y correctivas.
- Proporcionar actualizaciones de software, parches, hardware, servicios y/o soluciones alternativas adecuadas para resolver o mitigar (caso que no sea posible resolver) todas las vulnerabilidades asociadas con los Trenes y Equipos, manteniendo el nivel establecido de Seguridad de la Información y de los Sistemas de la Información.
- El adjudicatario deberá establecer un proceso de actualización de software siempre que sea posible.
- Informar de todas aquellas vulnerabilidades detectadas, y que puedan afectar a los sistemas de Metro de Madrid, fuera del ciclo de vida del contrato o del periodo de garantía. Y, en caso de conocerlas, indicar las medidas para mitigarlas.

## 5.11 Aceptación del sistema

Metro de Madrid podrá ejecutar auditorías y pruebas de seguridad durante las distintas fases del proyecto a fin de comprobar el cumplimiento de los requisitos de seguridad establecidos en el presente documento.

El incumplimiento de alguno de estos requisitos, podría implicar que no se acepte el paso a producción / operación del sistema de información.



## **6. Cualificaciones profesionales de Seguridad de la Información**

El adjudicatario, designará un Responsable de Seguridad que será la persona encargada de velar por el cumplimiento de los requisitos de ciberseguridad especificados en el presente documento durante toda la vigencia del contrato.

## **7. Mecanismos de coordinación en ciberseguridad**

Al inicio del proyecto, el adjudicatario y Metro de Madrid establecerán los mecanismos y procedimientos que se llevarán a cabo para garantizar la ciberseguridad de los Sistemas de Información objeto del contrato, así como también para cumplir con los requisitos indicados en el presente documento.