Universidad de Navarra

CLÁUSULAS DE SEGURIDAD APLICABLES A CONTRATISTAS CON ACCESO A LOS SISTEMAS DE INFORMACIÓN

A los efectos de estas cláusulas, se denominará “Sistema de Información de la Universidad de Navarra” al conjunto de software, hardware, infraestructuras y datos que dan soporte informático y de telecomunicaciones a los procesos de la Universidad de Navarra, tanto en las versiones en producción como versiones de desarrollo, test, pre-producción, o cualesquiera otras que fueran utilizadas en las distintas fases de la prestación de los servicios.

Con respecto al “Sistema de Información de la Universidad de Navarra”, el contratista deberá cumplir la normativa legal aplicable en materia de seguridad y privacidad de los sistemas de información, así como los requisitos que se detallan a continuación:

1. El contratista deberá definir, implementar y mantener una “Política de Seguridad de la Información”, aplicable a los servicios objeto del contrato, basada en la Política de Seguridad de la Información de la Universidad de Navarra, o que cumpla con las exigencias de la norma ISO/IEC 27001:2013. Dicha política será redactada de forma sencilla, precisa y comprensible, se mantendrá permanentemente actualizada y a disposición de la Universidad de Navarra, y deberá ser accesible a todos los miembros de la organización del contratista que intervengan en la prestación de los servicios.

2. En la fase de diseño de los servicios objeto del contrato, se realizará un estudio previo de las medidas de seguridad que se requieran para proteger los componentes del “Sistema de Información de la Universidad de Navarra” que intervengan en el desarrollo del presente contrato, de conformidad con la naturaleza de la información, el servicio prestado, las presentes cláusulas y los requerimientos de la normativa que les aplique, incluyendo el apartado 1.1.5 del Documento “Requisitos No Funcionales” de la Universidad de Navarra.

3. En todo caso, se establecen a continuación las condiciones y medidas mínimas en materia de seguridad de la información que el contratista deberá implantar y mantener para la prestación del servicio:

    a. Los empleados del contratista o las subcontratas, si las hubiera, que tengan acceso al “Sistema de Información de la Universidad de Navarra” o alguno de sus componentes, deberán estar previamente identificados por el contratista y autorizados nominalmente por la Universidad de Navarra.

b. El contratista mantendrá actualizada una relación de las personas anteriores, asociadas a las distintas funciones que realicen en el marco de los servicios prestados y a los perfiles de acceso al “Sistema de Información de la Universidad de Navarra”.

c. Esta relación indicará explícitamente, si fuera el caso, a aquellos usuarios que dispongan de privilegios de administración en el “Sistema de Información de la Universidad de Navarra” o alguno de sus componentes.

d. Existirá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que accede o intente acceder al “Sistema de Información de la Universidad de Navarra” o alguno de sus componentes, verificando que está autorizado y limitándose la posibilidad de intentar reiteradamente el acceso no autorizado.

e. De cada intento de acceso se registrará, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el tipo de acceso y si ha sido autorizado o denegado. Dicho registro se conservará como mínimo durante dos años. El contratista se encargará de revisar al menos mensualmente la información registrada y elaborará un informe de las incidencias detectadas si las hubiera.

f. Con una periodicidad no superior a un año se cambiarán las contraseñas asignadas a los empleados del contratista o las subcontratas, las cuales se almacenarán de forma ininteligible. No se habilitarán ni utilizarán las funcionalidades de las aplicaciones, navegadores o sistemas operativos que permitan guardar o recordar las credenciales de acceso de forma automática.

g. El contratista mantendrá las redes, los equipos y dispositivos de su propiedad desde los que acceda al “Sistema de Información de la Universidad de Navarra” debidamente actualizados y protegidos contra ciberamenazas.

h. Cuando el servicio prestado exija el acceso remoto al “Sistema de Información de la Universidad de Navarra”, se realizará mediante comunicaciones cifradas VPN o técnicas similares.

i. Exclusivamente las personas previamente autorizadas por la Universidad de Navarra podrán tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte al “Sistema de Información de la Universidad de Navarra”.

4. Para la realización de cambios o actualizaciones en el “Sistema de Información de la Universidad de Navarra”, así como, en su caso, la recuperación de datos o reversión de configuraciones, será necesaria la previa aprobación de la Universidad, siguiendo los procedimientos de Gestión de Cambios vigentes.

5. Los datos contenidos en el “Sistema de Información de la Universidad de Navarra”, así como la información sobre arquitectura de sus componentes, configuraciones, etc. a que tenga acceso el contratista o cualquiera de sus empleados o personal subcontratado, tendrán carácter de “información confidencial” y no podrán ser comunicados a un tercero bajo ningún concepto, sin el consentimiento previo de la Universidad de Navarra.

6. Cuando sea necesaria la comunicación de “información confidencial” entre la Universidad de Navarra y el contratista o sus subcontratistas, si los hubiera, se hará de forma cifrada.

7. Cuando sea del caso, en las fases de prueba y desarrollo se aplicarán a la “información confidencial” técnicas de seudonimización, enmascaramiento, entremezclado o similares encaminadas al tratamiento seguro de los datos.

8. Los soportes que contengan “información confidencial”, si los hubiera, deberán permitir identificar el tipo de información que contienen, estar cifrados, serán inventariados y solo serán accesibles por el personal involucrado en la prestación del servicio. La salida de soportes y documentos fuera de los locales de la Universidad de Navarra o del contratista deberá ser autorizada por la Universidad. Siempre que vaya a desecharse cualquier documento o soporte que contenga “información confidencial” se procederá a su destrucción o borrado seguro, adoptando las medidas necesarias para evitar el acceso a la información que contenía o su recuperación posterior, y registrando el proceso en el inventario.

9. A la finalización del contrato, según el criterio o indicación de la Universidad de Navarra, el equipo prestador del servicio procederá a destruir, devolver a la Universidad o transferir al proveedor que se le indique toda la “información confidencial” utilizada durante la prestación del servicio, independientemente del tipo de soporte en que se encuentre recogida, así como los propios soportes. La obligación de confidencialidad persistirá incluso después de terminada la relación contractual.

10. Queda expresamente prohibida:

    - La utilización del “Sistema de Información de la Universidad de Navarra” para actividades no autorizadas, ajenas a los servicios prestados, y/o que estén prohibidas por disposiciones legislativas o normativas.

    - El uso del “Sistema de Información de la Universidad de Navarra” o de alguna de sus partes para una finalidad distinta a la de su propósito.

    - La posesión, distribución, cesión, revelación o alteración de cualquier información sin el consentimiento expreso por escrito de la Universidad de Navarra.

    - La instalación o modificación no autorizada de hardware o software, la modificación de la configuración o conexión a redes o la reubicación física del “Sistema de Información de la Universidad de Navarra” o cualquiera de sus componentes.

    - La sobrecarga, prueba, o desactivación de los mecanismos de seguridad del “Sistema de Información de la Universidad de Navarra” o cualquiera de sus componentes.

    - La monitorización no autorizada de redes u otros recursos o componentes del “Sistema de Información de la Universidad de Navarra”.

    - La instalación o utilización de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, equipos u ordenadores portátiles, puntos de acceso inalámbricos, o dispositivos similares.

- Compartir cuentas e identificadores personales con otros usuarios, o permitir el uso de mecanismos de acceso, sean locales o remotos, a usuarios no autorizados.

11. El contratista dispondrá de un procedimiento de registro, notificación y gestión de las incidencias que afecten o puedan afectar al "Sistema de Información de la Universidad de Navarra" o cualquiera de sus componentes, en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hayan derivado de la misma y las medidas correctoras aplicadas. El contratista se obliga a comunicar a la Universidad de Navarra dichas incidencias a la mayor brevedad y en todo caso dentro del plazo máximo de 48 horas a contar desde que se ha detectado la incidencia, así como a mantenerla informada de las medidas aplicadas y de su evolución.

12. El contratista deberá implantar un Plan de Contingencia que permita garantizar la correcta operación y entrega de los servicios según los plazos y niveles de servicio especificados en el apartado correspondiente del presente contrato, incluso aunque se produzca alguna incidencia grave.

13. El contratista se compromete a formar e informar a su personal en las obligaciones que emanan de estas cláusulas y la normativa legal aplicable, para lo cual programará las acciones formativas necesarias y llevará un registro de las mismas, debiéndose acreditar el conocimiento y compromiso de la presente cláusula de seguridad por parte de todos los usuarios que intervengan en la prestación de los servicios.

14. La subcontratación de todo o parte de los servicios debe ser previamente autorizada por la Universidad de Navarra. El contratista será responsable del cumplimiento de lo especificado en esta cláusula por los posibles subcontratistas relacionados con la prestación de los servicios, si los hubiera.

15. El contratista implementará un proceso de revisión continua con el fin de detectar vulnerabilidades en los procesos y sistemas implicados en los servicios prestados a la Universidad de Navarra. Estas revisiones deberán realizarse al menos trimestralmente, poniendo a disposición de la Universidad de Navarra los resultados de las mismas.

16. El contratista podrá ser auditado por personal autorizado por la Universidad de Navarra en cualquier momento del desarrollo de los trabajos, previo aviso con 7 días de antelación, con el fin de verificar la seguridad implementada, comprobando que se cumplen las recomendaciones de protección y las medidas de seguridad de la distinta normativa, en función de las condiciones de aplicación en cada caso.

17. Cuando los servicios prestados por el contratista impliquen el tratamiento de datos personales, se estará, además, a lo convenido en el Contrato de Encargo de Tratamiento correspondiente, y tomará las medidas técnicas y organizativas apropiadas de conformidad con el Artículo 25 del Reglamento (UE) 679/2016 (Reglamento General de Protección de Datos).