

Norma de Seguridad: Código de Conducta Informático para entidades proveedoras

Rble. elaboración y mantenimiento:
Departamento de Seguridad

Revisión: 08

Fecha de entrada en vigor: 02/05/11

1. OBJETO	2. ALCANCE
El objetivo de esta Norma es establecer la política de Seguridad que ayude a las entidades proveedoras de Lantik a utilizar adecuadamente la infraestructura y recursos informáticos dispuestos por Lantik.	Es de aplicación a la infraestructura y recursos informáticos utilizados por las entidades proveedoras de Lantik, entre los que se incluyen los equipos informáticos, programas, servidores, redes, ubicaciones, etc. que posibilitan el uso de las herramientas informáticas, el acceso a otras redes (por ejemplo: Internet, intranet, red corporativa), la utilización de servicios corporativos como el correo electrónico, acceso a aplicaciones, etc.

ÍNDICE

1.	OBJETO	1
2.	ALCANCE	1
3.	INTRODUCCIÓN	2
4.	ÁMBITO DE APLICACIÓN	3
5.	MOTIVOS Y OBJETIVOS	4
6.	PAUTAS GENERALES SOBRE EL USO DE LOS RECURSOS INFORMÁTICOS	5
7.	TRATAMIENTO DE LA INFORMACIÓN	7
8.	FACULTAD DE REVISIÓN Y CONTROL	9
9.	ACCESO A LAS INSTALACIONES	10
10.	ACCESO A LA RED CORPORATIVA	11
11.	UTILIZACIÓN DE LOS EQUIPOS INFORMÁTICOS (HARDWARE)	13
12.	UTILIZACIÓN DE LOS PROGRAMAS Y DE LOS ARCHIVOS INFORMÁTICOS (SOFTWARE)	14
13.	NAVEGACIÓN EN INTERNET	16
14.	USO DEL CORREO ELECTRÓNICO	17
15.	ALMACENAMIENTO (UNIDADES DE RED, PUNTOS TRABAJO COLABORATIVO, ETC.)	18
16.	RECURSOS APORTADOS POR EL PROVEEDOR	19
17.	CUMPLIMIENTO	19
18.	PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y CONFIDENCIALIDAD	20
19.	NECESIDAD DE CUMPLIMIENTO DE LAS NORMAS DE CONDUCTA	22
20.	ENTRADA EN VIGOR Y VIGENCIA	23
21.	DOCUMENTOS RELACIONADOS	24
22.	HISTORIAL DE REVISIONES	24

3. INTRODUCCIÓN

3.0. Lantik dispone de infraestructura y recursos informáticos que garantizan la eficiencia y rapidez en la prestación de sus servicios. Entre estos instrumentos de trabajo se incluyen los equipos informáticos, programas, servidores, redes, etc. que posibilitan el uso de las herramientas informáticas, el acceso a otras redes (por ejemplo: Internet, intranet, red corporativa), la utilización de servicios corporativos como el correo electrónico, acceso a aplicaciones, etc.

3.1. Debido a la generalización del uso de tales recursos y a las responsabilidades asumidas por Lantik en su servicio a sus clientes, se impone la necesidad de establecer unas normas claras que ayuden a las entidades proveedoras a utilizar adecuadamente estos medios.

3.2. Definiciones

[Administradores](#)

[Actualización](#)

[BFA - DFB](#)

[CAU](#)

[Contraseñas](#)

[Cuenta de usuario o "User-id"](#)

[Direcciones de Internet](#)

[Entidad Proveedoradora](#)

[Información](#)

[Informática móvil](#)

[Infraestructura](#)

[Perfil Usuario](#)

[Perfil Administrador \(Secundario\)](#)

[Red \(de datos\)](#)

[Red Interna](#)

[Sistema de información](#)

[Usuario/a](#)

4. ÁMBITO DE APLICACIÓN

- 4.0. Las normas incluidas en el presente Código de Conducta Informático serán de aplicación a todas las entidades proveedoras de Lantik.
- 4.1. A los efectos del presente Código de Conducta Informático, se entenderá por proveedor a toda persona o empresa, no de plantilla, que provee servicios a Lantik o sus clientes, así como a cualquier persona externa que en virtud de cualquier relación tenga acceso a información o recursos de Lantik o sus clientes.
- 4.2. El Código de Conducta Informático resulta igualmente de aplicación para todas las comunicaciones realizadas a través de la red de Lantik, o los instrumentos y sistemas que, en su caso, la organización hubiera puesto a disposición de las entidades proveedoras.
- 4.3. En caso de que Lantik introduzca y ponga a disposición de las entidades proveedoras nuevos recursos, distintos a los previstos en el presente Código de Conducta Informático, y hasta que se facilite una regulación más precisa acerca de los mismos, se aplicará en cuanto a su uso se refiere lo dispuesto en el presente Código de Conducta Informático.
- 4.4. A las personas que administren infraestructuras o recursos informáticos de Lantik, adicionalmente les aplicarán las normas incluidas en el Anexo NSG 1/1 Norma Seguridad: Código de Conducta Informático. Anexo para Administradores, que será facilitado a los administradores por el Departamento de Seguridad.
- 4.5. Para la resolución de cualquier duda o consulta de carácter técnico que se le pueda plantear con relación al contenido del presente Código de Conducta Informático, rogamos lo consulte a través del CAU.

5. MOTIVOS Y OBJETIVOS

- 5.0. El establecimiento de las pautas contenidas en el presente Código de Conducta Informático viene motivado por la necesidad de establecer reglas claras que (i) garanticen un uso adecuado y eficiente de los sistemas e instrumentos técnicos e informáticos de trabajo que Lantik pone a disposición de las entidades proveedoras, (ii) eviten determinadas prácticas consistentes en la utilización incorrecta o inadecuada de los mismos y (iii) garanticen el cumplimiento por Lantik y las entidades proveedoras de las distintas disposiciones normativas que resultan de aplicación.
- 5.1. Asimismo, pretende concienciar a las entidades proveedoras sobre la seguridad de la información tanto dentro como fuera de las instalaciones de Lantik. Por ello, las normas y reglas del Código de Conducta Informático deben asimismo adoptarse en el supuesto de que el/la proveedor/a tenga acceso a la red corporativa desde ordenadores situados fuera de las instalaciones de Lantik.
- 5.2. El presente Código de Conducta Informático también pretende concienciar a las entidades proveedoras de Lantik de la necesidad de utilizar correctamente los recursos informáticos para garantizar los compromisos de calidad y confidencialidad que asumimos con terceros/as (administraciones, clientes, empresas, etc.) y con el resto de las entidades proveedoras, dado que Lantik ha adquirido un nivel de compromiso muy importante en este sentido respecto a su información, que no debe ser revelada ni estar disponible para terceras personas.
- 5.3. La introducción de las nuevas tecnologías de la información en el seno de nuestra organización incrementa exponencialmente los riesgos que se pueden generar ante cualquier eventual revelación de información fuera del entorno de Lantik. Este aspecto es esencialmente significativo en un entorno institucional y público como el de Lantik. En consecuencia, considerando el carácter sensible y confidencial del trabajo que se realiza, Lantik se ha dotado de sistemas de monitorización y supervisión de la utilización por parte de las entidades proveedoras de los instrumentos técnicos e informáticos existentes en el seno de Lantik.

6. PAUTAS GENERALES SOBRE EL USO DE LOS RECURSOS INFORMÁTICOS

- 6.0. Las pautas aquí descritas intentan precisar de forma clara y transparente el uso que debe hacerse de los recursos informáticos e infraestructura. Lantik está a la entera disposición de las entidades proveedoras para cualquier aclaración o duda que pueda surgir respecto del cumplimiento de las mismas.
- 6.1. Es propósito de Lantik dar cumplimiento al contenido de las leyes de la propiedad intelectual o industrial, por lo que las entidades proveedoras deberán comprobar, antes de utilizar y/o poner a disposición de Lantik, programas o información, si se encuentran protegidos por las leyes de la propiedad intelectual o industrial y citar siempre la fuente en el caso de que utilicen dicha información en cualquier documento de trabajo.
- 6.2. Lantik, podrá solicitar en cualquier momento la restitución o destrucción inmediata de cualquier clase de información que le haya sido revelada o haya sido creada por el proveedor.
- 6.3. Lantik, podrá auditar en cualquier momento, los recursos propios o ajenos que den soporte a los servicios contratados.
- 6.4. Las entidades proveedoras deberán mantener los medios puestos a su disposición en un estado de utilización óptimo, eliminando la información que consideren prescindible o sin valor, para mejorar el rendimiento y calidad de servicios de Lantik y garantizar la suficiente operatividad.
- 6.5. Los Recursos TI y la Información de Lantik que haya sido puesta a disposición de las entidades proveedoras, deberán ser reintegrados por estos en el momento en que Lantik así lo requiera, o en su defecto a la terminación, cualquiera que sea la causa, del trabajo o proyecto.

Gestión y comunicación de incidentes de seguridad

- 6.6. Los incidentes de seguridad de seguridad deberán ser identificados inmediatamente y reportados al CAU, atendiendo a los procedimientos establecidos, de modo que puedan llevarse a cabo acciones correctoras tan pronto como sea posible. A continuación, se exponen algunos casos de incidentes que deben ser reportados:
- Cualquier pérdida o daño de un Recurso IT o de Información de Lantik.
 - Compromiso o pérdida de contraseñas o claves de autenticación para el acceso a un Recurso IT o de Información de Lantik.
- 6.7. Si la entidad proveedora de Lantik es consciente de una debilidad o vulnerabilidad de seguridad en cualquier sistema de Lantik tiene la obligación de reportarla inmediatamente a través de los canales establecidos al efecto; faltar a la obligación de informar de ella puntualmente será considerado como un incidente de seguridad en sí mismo. Está terminantemente prohibido tratar de probar o explotar la debilidad o vulnerabilidad de seguridad que se hubiera detectado.
- 6.8. Lantik, se reserva el derecho a adoptar cualquier medida de seguridad oportuna cuando se le notifique o tenga indicios de que la entidad proveedora de Lantik sufra alguna vulnerabilidad.
- 6.9. Igualmente, en caso de que la entidad proveedora de Lantik sea consciente de una vulnerabilidad en sus propios sistemas, así como de la posibilidad de haber sido afectados por algún tipo de incidente de

seguridad, esta deberá reportar dicha circunstancia a Lantik de cara a que se tomen las medidas pertinentes para evitar una afección a los sistemas de Lantik.

Uso con finalidad profesional

- 6.10. Todos los medios puestos a disposición de las entidades proveedoras, por parte de Lantik, se entregan para ser utilizados con una finalidad exclusivamente profesional. No está permitido el almacenamiento de ningún tipo de información, documentación, etc., privada en los equipos informáticos profesionales.
- 6.11. Todas las conexiones que se produzcan a través de la red de Lantik (corporativa, Internet, etc.) serán utilizadas con una finalidad profesional.
- 6.12. Cualquier otro uso está prohibido.

Finalización de la relación con Lantik

- 6.13. Lantik pone a disposición de las entidades proveedoras los sistemas informáticos adecuados para la realización de sus funciones mientras se mantenga vigente la relación con ellos. A partir de la finalización de la colaboración con Lantik, no se podrá tener acceso a los equipos técnicos e informáticos y consiguientemente a los archivos incluidos en los mismos.
- 6.14. En el supuesto de que el/la proveedor/a tenga en su poder determinados medios o equipos informáticos (ordenador portátil, soportes, información, etc.), tendrá que devolverlos previamente a la finalización de su relación.
- 6.15. Asimismo, si un/a proveedor finaliza su relación con Lantik, el/la mismo/a deberá dejar intactos todos los archivos y documentos.
- 6.16. Las credenciales de acceso serán inhabilitadas cuando la entidad proveedora que autentican termina su relación con Lantik.
- 6.17. Las obligaciones con respecto a la protección de la confidencialidad, privacidad y propiedad intelectual (si la hubiere) subsistirán aún después de finalizar la relación con Lantik.

7. TRATAMIENTO DE LA INFORMACIÓN

- 7.0. Toda la información relacionada con las actividades de Lantik, exceptuando aquella información de carácter público, se considera de uso oficial, por lo que se obliga a los proveedores a utilizar la información única y exclusivamente con la finalidad de cumplir las funciones encomendadas, extremando las precauciones cuando se esté teletrabajando.
- 7.1. Las entidades proveedoras están obligadas a proteger, conservar y tratar con carácter confidencial toda la información corporativa y en particular y con carácter general, a no reproducirla, transformarla ni usarla de manera distinta a la que sea precisa para el ejercicio de sus funciones. Además, para el adecuado desempeño de sus funciones y obligaciones, las entidades proveedoras deberán, en todo caso, cumplir, por un lado, las medidas e instrucciones (técnicas y organizativas) de seguridad que se adopten por Lantik para proteger sus sistemas de información corporativos y, por otro lado, la normativa vigente en el ámbito de protección de datos y de seguridad de la información.
- 7.2. Los proveedores tienen conocimiento de que tanto la Información de Lantik como aquella obtenida en base a información relacionada con ella, serán propiedad exclusiva de Lantik, no pudiendo revelarla ni llevar a cabo una descarga o extracción de los recursos IT que no esté autorizada y justificada en el desarrollo de la actividad.
- 7.3. Los proveedores únicamente accederán o harán uso de cualquier Información de Lantik, así como de aquellos contenidos que estén bajo la responsabilidad, control y/o custodia de Lantik, con la obligación de cumplir con los términos de uso o licencia, copyright, o requerimientos especificados. Los proveedores no podrán copiar, distribuir, proporcionar o difundir en modo alguno los contenidos señalados, a aquellas personas no amparadas para ello por los términos de uso, licencia, copyright o requerimientos mencionados.
- 7.4. La entidad proveedora deberá mantener la Información, así como las copias de la misma, lo suficientemente segura como para impedir el acceso no autorizado de una tercera parte. Así mismo, acuerda no realizar copias ni reproducir de ningún modo la Información excepto para aquellos casos justificados y autorizados por la persona competente. Dichos casos no podrán, en ningún momento, contradecir lo indicado en el presente Código de Conducta.
- 7.5. Se debe mantener control y vigilancia respecto a la información en formato físico, especialmente aquella información con carácter confidencial o que contenga datos de carácter personal siguiendo en este caso lo indicado en el apartado "18PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y CONFIDENCIALIDAD" de este Código de Conducta Informático.
- 7.6. Las entidades proveedoras deben conocer y aplicar las medidas correspondientes a los distintos niveles de clasificación de la información, que se distinguen entre:
- Información de Uso Oficial:
 - Información Confidencial: Información sensible de Lantik cuya pérdida pudiera tener como consecuencia un menoscabo grave en la reputación o en las finanzas de Lantik y/o sólo deba ser conocida por las personas que justifiquen su acceso para el desempeño de sus funciones. Se incluyen dentro de este grupo los tratamientos que incluyan datos de carácter personal.

- Información Privada: Información cuya divulgación, compromiso o destrucción tendría directa o indirectamente un efecto adverso sobre Lantik o su personal. La mayor parte de la información se clasifica en este nivel.
 - Información Pública: Información no clasificada en alguno de los niveles anteriores. Esta información es la que Lantik pone a disposición del público dentro de su página Web o cualquier otro medio público (ofertas, prensa, etc.). También aquella información que sin haber sido comunicada previamente es de acceso público previa petición a la persona propietaria. Dentro de este grupo se incluye la información de contacto, información corporativa publicada, información del registro mercantil, publicidad de la empresa, etc.
- 7.7. Con carácter general, el intercambio de información por parte de los proveedores se realizará de acuerdo con lo establecido para su tipo de información, atendiendo, en cualquier caso, las peticiones y requisitos que pudiera realizarse por parte del personal de Lantik para dicho intercambio.
- 7.8. Con carácter general, cuando se digitalicen documentos el proveedor deberá ser especialmente cuidadoso con el almacenamiento, tratamiento y transmisión de las imágenes, especialmente si contienen Información Privada o Confidencial.

8. FACULTAD DE REVISIÓN Y CONTROL

- 8.0. Lantik se reserva la facultad de revisar los sistemas informáticos y controlar a través de los medios de que dispone la utilización que cada proveedor realiza de los medios y recursos informáticos puestos a su disposición, cuando se estime necesario para la protección de los intereses de Lantik y de los de los/as demás usuarios/as, o cuando resulte conveniente por razones específicas de seguridad o del servicio, garantizando en todo momento los principios de necesidad, minimización y proporcionalidad del tratamiento.
- 8.1. Los accesos a los sistemas de información podrán ser monitorizados y registrados para auditar el uso de los mismos.
- 8.2. Lantik, como Responsable de Tratamiento, informa a sus proveedores que sus datos serán tratados con la finalidad de securizar el acceso lógico a la infraestructura TI y gestionar ciberincidentes. Dicho tratamiento implica que puedan tratarse datos que permitan geolocalizar el acceso y el uso de los sistemas corporativos de Lantik. El tratamiento de los datos está legitimado en el desarrollo y ejecución de la relación contractual que le une al proveedor con Lantik.
- 8.3. Asimismo, Lantik podrá comunicar dichos datos a las Fuerzas y Cuerpos de Seguridad del Estado para casos de denuncias y/o requerimiento judicial y a Juzgados por requerimiento judicial. Puede consultarse en la web de Lantik mayor detalle sobre dicho tratamiento, así como información sobre los derechos de las personas interesadas.

9. ACCESO A LAS INSTALACIONES

- 9.0. Toda persona que acceda a las instalaciones de Lantik (sobre todo donde exista equipamiento esencial que forme parte del CPD) deberá cumplir la normativa de acceso aplicable.
- 9.1. Será necesario para el acceso a las instalaciones de Lantik que tengan implementado un sistema de control de accesos mediante tarjeta identificativa:
- Que se proporcione una tarjeta identificativa que deberá llevar siempre en un lugar visible.
 - Tras finalizar el servicio o visita, la tarjeta debe de ser devuelta en el puesto de vigilancia situado en la planta baja de Lantik.

Se registrará la información obtenida de los accesos mediante las tarjetas proporcionadas a los proveedores que vayan a acceder a las instalaciones de Lantik.

10. ACCESO A LA RED CORPORATIVA

- 10.0. Las personas usuarias del proveedor se adscribirán al contenido de las cláusulas de confidencialidad firmadas por el proveedor sobre su deber de confidencialidad y respeto a las políticas y procedimientos existentes.
- 10.1. Todas las cuentas de las entidades proveedoras deben tener definidas unas credenciales que consten de un nombre de usuario único, y una contraseña.
- 10.2. Las entidades proveedoras de Lantik deben cumplir las normas de seguridad aprobadas.
- 10.3. Ningún/a proveedor utilizará la Red Corporativa para proporcionar acceso a terceras personas o entidades.
- 10.4. Las empresas proveedoras aceptan las siguientes directrices en relación con la generación y gestión de contraseñas y se comprometen a su cuidado y diligencia en el cambio y custodia de las contraseñas. En este sentido, durante la generación y gestión de contraseñas, deberán tener en cuenta lo siguiente:
- Longitud: igual o superior a 8 caracteres.
 - Complejidad: no debe contener en parte o en su totalidad el nombre de usuario, y debe estar compuesta al menos por caracteres de tres de las siguientes cuatro categorías (minúsculas, mayúsculas, números y símbolos especiales).
 - Repetición: la contraseña no deberá coincidir con ninguna de las 8 últimas contraseñas utilizadas.
 - No deben contener partes significativas del nombre de cuenta del usuario o nombre completo.
 - Semántica: se deben evitar contraseñas basadas en repetición de caracteres, palabras del diccionario, secuencias simples (nombres de familiares o mascotas, matrículas, números de teléfono, etc.).
 - Número de intentos fallidos de acceso limitado: una vez se introduzca el usuario o contraseña de manera errónea tras 10 intentos fallidos de acceso, se bloqueará el equipo.
 - Precauciones: evitar apuntarlas en un papel, no enviarlas por medios electrónicos, no usar la misma contraseña para distintos servicios, desactivar la característica "Recordar la contraseña" de los navegadores y aplicaciones, etc.
 - Al igual que la contraseña de red, la contraseña de emergencia también debe de cumplir los criterios de complejidad.
 - Mantenerlas en secreto.
 - Reportar de forma inmediata en el caso de que haya evidencias o sospechas de que las credenciales se hayan visto comprometidas.
- 10.5. Como norma general, las entidades proveedoras deberán de cambiar las credenciales de acceso en el primer inicio de sesión.
- 10.6. Las credenciales de las entidades proveedoras serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

NCS-1 / 1



Norma de Seguridad: Código de Conducta Informático para entidades proveedoras

Revisión: 08

Fecha de entrada en vigor: 02/05/11

- 10.7. Las entidades proveedoras de Lantik deben comunicar todos los problemas que pudieran surgirles respecto a la utilización de la Red al CAU.
- 10.8. Este recurso se utilizará con una finalidad exclusivamente profesional.
- 10.9. Cualquier otro uso está prohibido.

11. UTILIZACIÓN DE LOS EQUIPOS INFORMÁTICOS (HARDWARE)**Principios generales**

- 11.0. Este recurso se utilizará con una finalidad exclusivamente profesional.
- 11.1. Cualquier otro uso está prohibido.
- 11.2. Con carácter general, se prohíbe la utilización de soportes con memorias extraíbles (por ejemplo: USB) por parte de las entidades proveedoras de Lantik salvo excepciones debidamente justificadas por la gestión operativa de Lantik.
- 11.3. Está expresamente prohibido el acceso o entrada por cualquier medio en los sistemas informáticos de otros/as usuarios/as utilizando una clave de identificación personal (login) o contraseña (password) de otro/a usuario/a.
- 11.4. Siempre que, por cualquier motivo, un/a proveedor abandone su puesto de trabajo bloqueará su sistema para evitar que ninguna persona no autorizada pueda acceder a información de Lantik que pudiera encontrarse albergada en el equipo del proveedor.
- 11.5. Respecto al control y revisión por parte de Lantik del buen uso que de los medios y equipos informáticos (hardware) realizan las entidades proveedoras, será de aplicación lo contenido en las cláusulas 8.1 y 8.2 del presente Código de Conducta Informático.

12. UTILIZACIÓN DE LOS PROGRAMAS Y DE LOS ARCHIVOS INFORMÁTICOS (SOFTWARE)**Principios generales**

- 12.0. En cualquier caso, la información de categorizada como USO OFICIAL, no podrá enviarse a través de ningún medio a terceras personas u organizaciones distintas de las receptoras de la información, salvo que la misma se ampare en las normas generales de aplicación en Lantik.
- 12.1. Los programas y archivos informáticos puestos a disposición de las entidades proveedoras de Lantik están destinados a un uso profesional.
- 12.2. En relación al control y revisión del uso de los programas y de los archivos informáticos por parte de las entidades proveedoras, serán de aplicación las cláusulas 8.1 y 8.2 del presente Código de Conducta Informático.

Seguridad en los programas y archivos informáticos

- 12.3. Todos los equipos utilizados para la prestación del servicio deben tener instalado un programa antivirus. No obstante, dado que estos programas antivirus no eliminan por completo el riesgo de generar y propagar un virus informático, el/la proveedor deberá tener la máxima diligencia a la hora de ejecutar archivos procedentes de fuentes no conocidas. En caso de duda, rogamos se abstenga de ejecutar el archivo o programa y contacte directamente con el CAU.
- 12.4. Bajo ninguna circunstancia se permite a las entidades proveedoras desactivar el programa antivirus instalado en los equipos.

Seguridad en la grabación de videoconferencias

- 12.5. Lantik podrá realizar grabaciones de las reuniones mantenidas con la entidad proveedora. El tratamiento de los datos está legitimado por ser necesario para el desarrollo y ejecución de la relación contractual con la entidad proveedora o, en su caso, por el consentimiento otorgado por esta.
- 12.6. Cuando se vaya a grabar la reunión o llamada, la persona encargada de convocarla debe informar al resto de personas participantes, y, de forma excepcional y solamente cuando la grabación de la reunión quede fuera de las funciones de los participantes de la reunión o llamada, se deberá solicitar adicionalmente el consentimiento de las personas participantes.
- 12.7. Se debe de limitar el número de personas convocadas, evitando el reenvío a grupos o listados genéricos y la reutilización de los códigos/enlaces de acceso. El acceso a esta grabación deberá estar restringido a las personas que lo requieran, delimitando en todo caso el tiempo de su almacenamiento.
- 12.8. La entidad proveedora debe ser diligente en el uso de los medios, especialmente con aquellos relacionados con la compartición de pantalla, vídeo o activación del micrófono; y aplicar buenas prácticas como la activación de la sala de espera o tener inhabilitados la cámara y el micrófono por defecto, apagar micrófono y cámara del ordenador siempre que sea necesario ausentarse de la reunión momentáneamente, difuminar el fondo o compartir siempre la aplicación y no la pantalla, entre otras.

NCS-1 / 1



Norma de Seguridad: Código de Conducta Informático para entidades proveedoras

Revisión: 08

Fecha de entrada en vigor: 02/05/11

12.9. La información adicional sobre el tratamiento de los datos personales se encuentra en el aviso legal publicado en la web de Lantik.

13. NAVEGACIÓN EN INTERNET**Principios generales**

- 13.0. En ningún caso debe accederse a direcciones de Internet de juegos, de contenido sexual, o que resulten ofensivas o atentatorias contra la dignidad humana o los derechos fundamentales. Asimismo, se deberá evitar visitar sitios no oficiales, poco conocidos o de dudosa reputación, para descargar cualquier información o software.
- 13.1. Este recurso se utilizará con una finalidad exclusivamente profesional.
- 13.2. Cualquier otro uso está prohibido.
- 13.3. Lantik podrá controlar y revisar los datos de las conexiones a la red de Internet desde los ordenadores utilizados por las entidades proveedoras en el desempeño de sus funciones, así como el contenido concreto de dichas conexiones, conforme lo establecido en las cláusulas 8.1. y 8.2 del presente Código de Conducta Informático.

14. USO DEL CORREO ELECTRÓNICO**Correo electrónico profesional**

- 14.0. Salvo excepciones debidamente justificadas y autorizadas, Lantik no proporciona recursos de este tipo a las entidades proveedoras.
- 14.1. La entidad proveedora a la que se le haya habilitado acceso a cuentas de correo electrónico corporativas debe evitar emitir comentarios despectivos u ofensivos, ni opiniones personales de carácter político, religioso o ideológico, etc., tales opiniones son personales y no deben representar a Lantik. También se deberá evitar la crítica de forma irresponsable sin argumentos, o discusiones y debates a través de estos medios.
- 14.2. El trato confidencial que requiere la relación entre Lantik y sus clientes o potenciales clientes implica necesariamente la utilización de los sistemas de comunicación más apropiados en relación con la naturaleza de la comunicación a realizar. Por este motivo:
- 14.2.1. Además de garantizar el cumplimiento de la normativa aplicable, uso adecuado y la seguridad, implica necesariamente que el contenido de las comunicaciones deba ser auditable y controlable por parte de los servicios técnicos de Lantik.
- 14.2.2. El intercambio de información entre Lantik y sus proveedores se producirá de modo seguro (cifrada) para la información clasificada tanto como Privada, así como Confidencial.

Principios generales aplicables al correo electrónico profesional

- 14.3. Para impedir las fugas de información y garantizar la eficacia del servicio, se evitará el envío innecesario de correos, limitando el número de destinatarios al estrictamente necesario.
- 14.4. Se prohíbe expresamente la interceptación y/o uso no autorizado de mensajes o direcciones de correo electrónico de otros/as usuarios/as del sistema informático de Lantik.
- 14.5. Las entidades proveedoras de Lantik deben rechazar cualquier mensaje de correo electrónico que provenga de fuentes no fiables, ya que podría contener virus o códigos maliciosos, contenido SPAM, etc.
- 14.6. Las entidades proveedoras de Lantik, evitarán la divulgación innecesaria de la dirección de correo, principalmente no participando en cadenas de mensajes, por altruista que pueda parecer su objetivo.
- 14.7. Las entidades proveedoras que hagan uso del correo electrónico deben seguir las normas y políticas establecidas para garantizar la confidencialidad e integridad en el intercambio de la información.
- 14.8. Respecto al control y revisión por parte de Lantik del buen uso que del correo electrónico realizan las entidades proveedoras, será de aplicación lo contenido en las cláusulas 8.1. y 8.2 del presente Código de Conducta Informático.

15. ALMACENAMIENTO (Unidades de red, puntos trabajo colaborativo, etc.)

- 15.0. El almacenamiento a disposición de las entidades proveedoras de Lantik están destinadas a un uso exclusivamente profesional.
- 15.1. En ningún caso puede hacerse uso del almacenamiento puestas a disposición de las entidades proveedoras para proceder al almacenamiento de datos privados o no profesionales.
- 15.2. Se deberán utilizar como unidades de trabajo colaborativas, las herramientas de Office 365, teniendo en consideración los accesos pertinentes.
- 15.3. Se prohíbe cualquier otro uso.
- 15.4. Las entidades proveedoras que utilicen estos recursos deben seguir las normas y políticas establecidas para garantizar la confidencialidad e integridad en el intercambio de información.
- 15.5. Respecto al control y revisión por parte de Lantik del buen uso de las unidades de red (almacenamiento) que realizan las entidades proveedoras, será de aplicación lo contenido en las cláusulas 8.1. y 8.2 del presente Código de Conducta Informático.

16. RECURSOS APORTADOS POR EL PROVEEDOR

- 16.1. Este apartado se aplica a los recursos aportados por el proveedor para la prestación del servicio.
- 16.2. Antes de su incorporación a la infraestructura de Lantik, debe de:
 - 16.2.1. Comunicar y contar con la aprobación del responsable del servicio de Lantik.
 - 16.2.1.1. Este la trasladará a Políticas Tecnológicas para su aprobación o denegación.
 - 16.2.1.2. En caso de aprobación debe de contar con la aprobación del Departamento de Seguridad de Lantik.
 - 16.2.1.3. Los recursos no se incorporan, hasta recibir el visto bueno del Dpto. de Seguridad. Esta incorporación puede suponer la implantación de controles propuestos por el Departamento de Seguridad.
- 16.3. Todos los equipos de la entidad proveedora que quieran incluirse al dominio de Lantik serán sometidos a un proceso de escaneo de vulnerabilidades que deberán superar para habilitar su inclusión. Igualmente, se deberá acreditar que se dispone de antivirus actualizado y proporcionar evidencia de la versión del sistema operativo.
- 16.4. Las empresas colaboradoras de Lantik deberá cumplir con las normas de protección de la propiedad intelectual usando en todo momento software legal, y manteniendo un inventario de las licencias del software instaladas.
- 16.5. Lantik se reserva el derecho de auditoría sobre los recursos aportados por parte de la entidad proveedora (auditorías de seguridad, informes de hacking ético, renovación de certificaciones de seguridad, el suministro de materiales que aseguren el uso de componentes cualificados conforme al Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional (CCN) o que estén certificados, etc.).
- 16.6. Para el establecimiento de las conexiones para los intercambios de información y prestación de servicios con otros sistemas, éstas deberán ser objeto de una autorización previa, estando prohibido cualquier flujo de información que no esté aprobado de forma expresa.
- 16.7. Para el establecimiento de la mencionada interconexión, se aceptarán las directrices de seguridad que Lantik considere oportunas.
- 16.8. Para conectarse a la red corporativa de forma remota, se deberá emplear siempre dispositivos que cumplan con las directrices de seguridad definidas por Lantik. Lantik se reserva la facultad de revisar las conexiones remotas y controlar a través de los medios de que dispone la utilización que cada usuario/a realiza de dichas conexiones y recursos informáticos puestos a su disposición, cuando se estime necesario para la protección de los intereses de Lantik y de los de los/as demás usuarios/as, o cuando resulte conveniente por razones específicas de seguridad o del servicio.

17. CUMPLIMIENTO

- 17.1. Es de obligación que las entidades proveedoras den cumplimiento a la legislación aplicable, como por ejemplo la normativa de protección de datos, ENS, LPI, LSSI, etc.

18. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y CONFIDENCIALIDAD

- 18.1. Es responsabilidad de las entidades proveedoras de los medios informáticos de Lantik que accedan a esta información, conocer y cumplir las medidas dispuestas en el RGPD
- 18.2. Cuando el producto o servicio contratado por parte de Lantik al proveedor implique el tratamiento de datos personales de este segundo por cuenta de Lantik, el proveedor tendrá consideración de encargado del tratamiento, quedando obligado al cumplimiento íntegro de la normativa en materia de protección de datos personales, así como de las obligaciones fijadas en el pliego o contrato menor que los vincule, tratando los datos personales únicamente para las finalidades acordadas y bajo las indicaciones de Lantik, que tendrá capacidad de supervisión del cumplimiento de las mismas.
- 18.3. En caso de violación de la seguridad de los datos personales en los sistemas de información utilizados por el Encargado del Tratamiento para la prestación de los servicios contratados, el Encargado del Tratamiento deberá notificar a Lantik, sin dilación indebida, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia conforme a lo dispuesto en el artículo 33.3 del RGPD.
- 18.4. La normativa de protección de datos otorga a las personas físicas, entre las que está el personal de las entidades proveedoras de Lantik, derechos que pueden ejercer ante la persona responsable del tratamiento, siendo los siguientes: el derecho de acceso, de rectificación, de supresión, de oposición, de limitación del tratamiento y el derecho a no ser objeto de decisiones individuales automatizadas y portabilidad, en su caso.
- 18.5. Los proveedores están expresamente obligados a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudieran conocer con ocasión del cumplimiento de su función, especialmente los datos personales, que no podrán copiar o utilizar con fin distinto al que esté determinado, ni tampoco ceder a otros ni siquiera a efectos de conservación. Este deber de confidencialidad persistirá aun cuando haya terminado la relación que les une a Lantik.
- 18.6. El personal de las entidades proveedoras deberá tratar la información a la que acceda para la ejecución del contrato de manera que se garantice en todo momento su confidencialidad. Esto implicará que deberá evitarse dejar la información o los documentos que la contengan en ubicaciones a la vista de personas ajenas sin supervisión, así como que los lugares donde se almacene guarden o conserve la información deberán ser aptos para garantizar el deber de confidencialidad.
- 18.7. Las entidades proveedoras deberán certificar que tanto el personal a su cargo como las personas subcontratistas y el personal al cargo de estas ha firmado una cláusula de confidencialidad por la cual se compromete a:
- No revelar la información que conozca en función de su cargo o cometido durante la prestación del contrato y posteriormente al mismo.
 - Conocer las medidas de seguridad tendentes a garantizar el cumplimiento de la política de seguridad de la información y de protección de los datos personales.

- 18.8. La entidad proveedora comunicará a Lantik toda filtración de información de la que tenga o llegue a tener conocimiento, producida por la vulneración del indicado acuerdo de confidencialidad de las personas que hayan accedido a la información. Tal comunicación no exime a la entidad proveedora de su responsabilidad, pero si la incumple dará lugar a cuantas responsabilidades se deriven de dicha omisión en particular.
- 18.9. Cuando el contrato no requiera el acceso al sistema de información de Lantik pero suponga el acceso a sus instalaciones, la empresa proveedora se compromete a mantener plena confidencialidad de la información que pudiera conocer de manera accidental por los accesos a las instalaciones, y especialmente, aquella que pueda suponer un riesgo para Lantik y/o para terceros en caso de ser conocida y/o pueda suponer una brecha de seguridad.
- 18.10. Los proveedores, una vez finalicen la relación con Lantik, deberán destruir o devolver, bajo el método acordado, los datos de carácter personal pertenecientes a Lantik y que pudieran estar bajo su control, así como cualquier otro soporte o documento en que conste algún dato personal. Las obligaciones de confidencialidad subsistirán aún después de finalizar la relación con Lantik.
- 18.11. Queda prohibida la salida de información propiedad de Lantik obtenida de sus sistemas de información o de otras fuentes, por cualquier medio físico o telemático, salvo autorización de Lantik.

19. NECESIDAD DE CUMPLIMIENTO DE LAS NORMAS DE CONDUCTA

- 19.1. Para requerir el cumplimiento debido a las políticas, normas y procedimientos que sean de aplicabilidad a los proveedores de los servicios, en el cumplimiento de sus responsabilidades, se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad,
- 19.2. A su vez, Lantik considera conveniente recordar a las entidades proveedoras la necesidad de que las mencionadas pautas sean seguidas fielmente por parte de los/las mismos/as, con el fin de salvaguardar la intimidad de clientes y usuarios/as, mejorar la calidad y capacidad de la red de comunicaciones y mejorar la seguridad.
- 19.3. Por ello, de no cumplirse por parte de las entidades proveedoras las pautas contenidas en el presente documento, Lantik se verá obligada a ejercer las medidas oportunas, a través de las pautas de resolución de incidentes al efecto. Todo ello sin perjuicio de posibles responsabilidades civiles, penales o laborales en las que hubiera podido incurrir el/la proveedor/a infractor/a.
- 19.4. Además, Lantik podrá interrumpir el servicio en el ordenador o dispositivo red, así como proceder al bloqueo de los usuarios del proveedor que haya realizado un uso de los medios técnicos e informáticos proporcionados por Lantik que no se adecue a lo establecido en el presente Código de Conducta Informático.
- 19.5. Las personas usuarias de las empresas proveedoras deberán recibir formación y participar en actividades de concienciación en materia de seguridad.
- 19.6. Estas acciones estarán centradas en el recordatorio de la normativa de seguridad aplicable, así como sobre las principales amenazas en la que los usuarios puedan verse involucrados.
- 19.7. También tendrán en cuenta la identificación y reporte de incidentes o actividades sospechosas que puedan ser constitutiva de riesgo para los sistemas de información de Lantik y la manera de informar de ellos.

20. ENTRADA EN VIGOR Y VIGENCIA

- 20.1. El contenido del presente Código de Conducta Informático es de obligatorio conocimiento y cumplimiento para todas las entidades proveedoras de Lantik. Su contenido entró en vigor el 02 de mayo del 2011 y se mantendrá en vigencia hasta tanto no sea modificado o reemplazado por otro.
- 20.2. Lantik pone a disposición de cada una de las entidades proveedoras una copia del mismo en http://lantik.bizkaia.eus/ca_contratacion.asp.
 - 20.2.1. En esta dirección estará en cada momento la última versión disponible.
- 20.3. Será responsabilidad del proveedor divulgar este Código de Conducta Informático en su organización.

21. DOCUMENTOS RELACIONADOS

NCS-1/2 Normativa de Seguridad de la Información para entidades proveedoras

Anexo NSG 1/1 Norma Seguridad: Código de Conducta Informático. Anexo para personal Administrador.

22. HISTORIAL DE REVISIONES

Revisión	Fecha	Modificaciones
00	24/03/11	Aprobación de la Norma
01	20/10/11	<ul style="list-style-type: none"> Se revisan en el apartado 3.3 las definiciones de Usuario y Administrador y se añaden definiciones para el Perfil Usuario y Perfil Administrador. Se incluye en el apartado 4 <i>Ámbito de Aplicación</i> un punto para indicar que las personas con perfil de administrador, adicionalmente les aplicarán las normas incluidas en el <i>Anexo NSG 1/1 Norma Seguridad: Código de Conducta Informático. Anexo para Administradores</i>, que les facilitará el Departamento de Seguridad.
02	10/05/13	<ul style="list-style-type: none"> Se añade al alcance del documento las ubicaciones. Se añade el apartado de acceso a las instalaciones. Se añade la obligatoriedad de portar tarjeta identificativa de forma visible siempre que se permanezca dentro de las instalaciones de Lantik. Se elimina el periodo transitorio de la versión 01(Título 18).
03	29/11/16	<ul style="list-style-type: none"> Se agrega cumplimiento principalmente de ENS Modificaciones menores respecto a la entrega de soportes, ya no se da intercambio de soportes. Se ajusta la política del correo electrónico para prohibir recursos de correo corporativo. Se mejora el procedimiento para incorporar RECURSOS APORTADOS POR EL PROVEEDOR Se elimina la necesidad de entregar copia, estará a disposición de las entidades proveedoras en http://lantik.bizkaia.eus/ca_contratacion.asp Se cambia título "Unidades de red" a "Almacenamiento" para incorporar nuevos tipos repositorios de información tipo red, SharePoint, etc. Se introduce nuevo título "RECURSOS NO SOLICITABLES POR PROVEEDORES" para incorporar nuevas políticas de seguridad de Lantik, como no VPN, no Intranet, etc. Se incluye procedimiento de excepciones.
04	21/09/18	<ul style="list-style-type: none"> Adecuación de la norma al RGPD: Se eliminan las referencias a la LOPD y se revisa el apartado 17. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. Se actualiza el documento según la nueva estructura organizativa y lenguaje neutro.
05	05/06/20	<ul style="list-style-type: none"> Se elimina el punto 7.2 en el que se referenciaba al comité de control informático, ya que se ha acordado que no es necesario.
06	14/10/22	<ul style="list-style-type: none"> Se amplía el punto 7.1 y se incluye los puntos 7.2 y 7.3 acorde al tratamiento "Control y seguridad de accesos lógicos"

Norma de Seguridad: Código de Conducta Informático para entidades proveedoras

Revisión: 08

Fecha de entrada en vigor: 02/05/11

07	18/09/23	<ul style="list-style-type: none"> • Se amplía el contenido de, "Pautas generales sobre el uso de los recursos informáticos", "Facultad de revisión y control", "Protección de datos de carácter personal y confidencialidad", incluyendo previsiones sobre confidencialidad en relación a las conexiones. • Se añade el apartado "Gestión y comunicación de incidentes de seguridad" • Se añade el apartado "Tratamiento de la información". • Se añaden comentarios a las cláusulas de cumplimiento, de interconexión de sistemas en "Recursos aportados por el proveedor". • Se hace referencia en el apartado "Pautas generales sobre el uso de los recursos informáticos" al reconocimiento de la aceptación y obligación por parte del usuario externo sobre las credenciales proporcionadas. • Se añade en el apartado "Utilización de los equipos informáticos (Hardware)" la prohibición de uso del USB o memorias extraíbles, salvo casos justificados por necesidades de la operación diaria • Se añade en el apartado de "Acceso a la red corporativa" las características que deberá de cumplir la contraseña utilizada, así como la puntualización del cambio de contraseña en el primer inicio de sesión.
08	02/01/24	<ul style="list-style-type: none"> • Se incluye cláusula informativa del tratamiento de la imagen de las personas proveedoras en la grabación de videoconferencias en el apartado 12.5. y siguientes