Lantik / BFA DFB Bizkaiko Foru Aldundia / Diputación Foral de Bizkaia	**NCS-1 / 2**

Normativa de Seguridad de la Información para entidades proveedoras

Rble. elaboración y mantenimiento: Departamento de Seguridad	Revisión: **01**
	Fecha de entrada en vigor: **02/05/11**

1. OBJETO	2. ALCANCE
Establece la normativa de seguridad de la información aplicable a las entidades proveedoras que presten servicios a Lantik.	Entidades proveedoras de servicios de Lantik.

ÍNDICE

3. La Seguridad de la Información para Lantik

La importancia de la Seguridad de la Información para Lantik

La información, así como las personas, los procesos, sistemas, redes, etc. que la soportan son considerados activos importantes. La disponibilidad, integridad, confidencialidad, autenticación y trazabilidad de la información, y de los activos que la soportan, son esenciales para mantener la seguridad de la información, el cumplimiento de la legalidad vigente, la competitividad, y la buena imagen para con los clientes.
Para lograr una adecuada seguridad de la información es imprescindible la gestión de la misma apoyándose en unas normativas y procedimientos adecuados a cumplir por todas las personas que actúan sobre activos de Lantik en el desarrollo de sus funciones.

Objetivos de la Normativa de Seguridad de la Información

Los objetivos globales de la Normativa de Seguridad de la Información son los siguientes:

- ***Marco Jurídico***

  Se adquiere el compromiso de **velar por el cumplimiento de la legislación vigente** en materia de protección y seguridad de la información y de los sistemas aplicable a todos sus procesos de negocio.

- ***Marco Normativo***

  Cumplimiento de las obligaciones contractuales establecidas tanto con clientes como entidades proveedoras, en relación a la seguridad de la información.

  Cumplimiento de los requisitos y buenas prácticas de Seguridad de la Información incluidas en las Normas ISO27001 e ISO27002.

4. Organización de la normativa, revisión y actualización

Esta normativa será revisada periódicamente. No obstante, debido a la propia evolución de la tecnología, las amenazas en relación a la seguridad de la información y a las nuevas obligaciones legales en la materia, Lantik se reserva el derecho a modificar esta normativa cuando sea necesario. Los cambios realizados serán divulgados a todas las partes interesadas mediante la publicación en la página web de lantik y la notificación de la nueva versión mediante correo electrónico por parte del CAU. Es responsabilidad de todo el personal que desarrolle actividades para Lantik, la lectura, conocimiento y cumplimiento de esta Normativa de Seguridad de la Información para entidades proveedoras.

5. Incumplimiento de la Normativa de Seguridad de la Información

Lantik se reserva el derecho adoptar las medidas que se consideren pertinentes en relación a la empresa contratada, y que pueden llegar a la resolución de los contratos que se tenga vigentes con dicha empresa.

6. Aspectos organizativos de la seguridad de la información

Objetivos

- Mantener la seguridad de la información sobre los activos de información de Lantik que son objeto de acceso, tratamiento, comunicación o gestión por entidades proveedoras de servicio.

1. Entidades proveedoras

.1 Los acuerdos (contratos) que impliquen acceder, procesar, comunicar o gestionar la información de la organización o los servicios de procesado de información, o añadir productos o servicios a los servicios de procesado de información, indicarán los controles de seguridad requeridos por parte de Lantik previa a la prestación del servicio.

7. Gestión de activos

Objetivos

- Establecer y mantener una protección adecuada a los activos de Lantik
- Asegurar que la información recibe un nivel adecuado de protección

1. Responsabilidades sobre los activos

.1 Se cumplirán, por parte dla entidad proveedora, las normas de uso aceptable de los activos establecidas por Lantik en su gestión de la seguridad de la información.

Norma Interna NCS-1/1 Norma de Seguridad: Código de Conducta Informático para Entidades proveedoras

2. Clasificación de la información

.1 **Toda la información relacionada con las actividades de Lantik se considera confidencial**. La entidad proveedora deberán cumplir las funciones y obligaciones aplicadas a la utilización de los sistemas de información según la normativa establecida por Lantik.

.2 Se garantizará el manejo de de la información de acuerdo al criterio de clasificación establecido.

8. Seguridad física y ambiental

Objetivos

- Prevenir e impedir accesos no autorizados, daños e interferencia a las instalaciones e información de Lantik.
- Proteger los sistemas de Lantik, ubicándolos en áreas protegidas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
- Contemplar la protección de los sistemas de Lantik en su traslado y permanencia fuera de las áreas seguras, por motivos de mantenimiento u otros.
- Controlar los factores externos o del entorno que pudieran perjudicar el correcto funcionamiento de los sistemas de información que albergan la información de Lantik.
- Implementar medidas para proteger la información manejada por el personal, en el marco normal de sus labores habituales.

1. Áreas seguras

.1 Se utilizarán correctamente los controles físicos de entrada establecidos para asegurar que únicamente accede el personal autorizado a los espacios de los que dispone Lantik: oficinas, despachos e instalaciones.

.2 Se seguirán las directrices y medidas de protección establecidas por Lantik contra las posibles amenazas externas y de origen ambiental.

.3 Se cumplirán las directrices establecidas para trabajar en las áreas protegidas.

.4 Llevar la identificación mientras permanezcan en instalaciones de Lantik.

2. Seguridad de los equipos

.1 La infraestructura tecnológica se ubicará en emplazamientos securizados y protegidos con el fin de reducir los riesgos derivados de las amenazas externas.

.2 Se protegerá la infraestructura tecnológica, que así lo necesite, contra fallos de provisión en el suministro eléctrico.

.3 La conexión de cualquier equipamiento a los circuitos tanto eléctrico como de comunicaciones estará previamente validado, con el fin de evitar interceptaciones o daños.

.4 Se deberá solicitar validación previa y se implementarán medidas de control indicadas, sobre toda la infraestructura que por necesidades puntuales se tenga que ubicar fuera de las áreas protegidas en Lantik o fuera de la organización.

.5 Salvo en aquellos casos en que se reciba actualización expresa, se prohíbe sacar de las instalaciones cualquier infraestructura TIC o software propiedad de Lantik

9. Gestión de comunicaciones y operaciones

Objetivos

- Garantizar el funcionamiento correcto y seguro de los activos que ofrecen los diferentes servicios a Lantik.
- Establecer responsabilidades y facilitar procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta ante incidentes y separación de funciones.

1. Responsabilidades y procedimientos de operación

.1 Lantik facilitará, en función de las necesidades identificadas, procedimientos de operación actualizados a las entidades proveedoras que los necesiten.

.2 Se prohíben los cambios sobre las infraestructuras y los recursos.

.3 Se definirán áreas de responsabilidad y tareas de manera segregada en los contratos de relación y en los acuerdos de nivel de servicio que se establezcan, con el fin de evitar modificaciones no autorizadas.

.4 Se deberá garantizar, en función del servicio prestado por la entidad proveedora, la utilización correcta de los entornos de desarrollo y pruebas.

2. Gestión de la provisión de servicios

.1 Se realizarán por parte de Lantik, controles para verificar que los requerimientos de seguridad establecidos de forma previa a la prestación de servicio han sido implementados y se mantienen en el tiempo correctamente.

.2 Los servicios prestados serán supervisados y revisados periódicamente. En función del tipo de servicio se podrán establecer auditorías de cumplimiento.

.3 En función de la criticidad y/o riesgo del servicio contratado, los cambios en la provisión del mismo deberán ser validados previamente por Lantik.

3. Planificación y aceptación del sistema

.1 Se establecerá una supervisión de la utilización de los recursos propiedad de Lantik empleados por la entidad proveedora, con el fin de garantizar una correcta capacidad de los mismos tanto en el presente mediante su monitorización, como en el futuro mediante el análisis de tendencias.

.2 Se establecerán criterios de aceptación para nuevos sistemas o la modificación de los existentes, realizadas por entidades proveedoras. En los entornos de desarrollo y prueba se realizarán las pruebas que garanticen un correcto paso al entorno de producción. Únicamente tras una aceptación formal se migrará al entorno de producción.

4. Protección contra código malicioso y descargable

.1 Se prohíbe la ejecución de código no autorizado. La configuración de los equipos garantizará que el código autorizado funciona de acuerdo con lo definido en la normativa establecida al respecto.

5. Gestión de la seguridad de las redes

.1 No se evitarán los mecanismos y actividades de gestión establecidos por Lantik que permitan proteger frente a las amenazas que les puedan afectar las redes y a las aplicaciones que las utilizan.

.2 Se identificarán tanto las características de seguridad, los niveles de servicio y los mecanismos de gestión para garantizar la seguridad del servicio de red prestados por entidades proveedoras.

6. Manipulación de los soportes

.1 La utilización de soportes extraíbles de información deberá ser validada previamente por Lantik y con la finalidad exclusiva recogida en el contrato de relación.

.2 A la finalización de la relación contractual con Lantik, los soportes extraíbles facilitados a la entidad proveedora para el desarrollo de sus funciones, deberán ser devueltos.

.3 El uso y almacenamiento de información en soportes extraíbles y la manipulación de los soportes estará regulado mediante la normativa establecida en Lantik.

.4 Se prohíbe el acceso a la documentación de Lantik, ubicada tanto en repositorios automatizados como no automatizados, a la que no se haya dado acceso expreso para el fin descrito en la prestación del servicio contratado.

7 Intercambio de información

.1 Sobre los intercambios de información realizados entre la entidad proveedora de servicio y Lantik se establecerán, en función de la criticidad considerada por Lantik, controles normativos, procedimentales y técnicos que protejan el intercambio de dicha información.

.2 El intercambio de información y el tratamiento de la misma, quedará regulado mediante el correspondiente acuerdo o contrato de relación entre Lantik y la entidad proveedora receptor de la misma.

.3 En los casos en los que la prestación del servicio incluya el tránsito de información, se implementarán por parte dla entidad proveedora los controles normativos y técnicos que eviten el uso indebido o el deterioro de la misma. Lantik se reservará el derecho de auditar estos controles o requerir la implantación de protecciones adicionales.

.4 Lantik podrá requerir que la información transmitida mediante mensajería electrónica esté adecuadamente protegida por parte dla entidad proveedora, requiriendo el cumplimiento de una normativa específica y/o la implementación de controles técnicos auditables.

.5 Se prohíbe la transmisión de información de Lantik a otras organizaciones. En caso de necesidad para la prestación del servicio contratado, la entidad proveedora de servicio deberá solicitar a Lantik validación previa a la transmisión de dicha información. En función de los niveles de clasificación y los requerimientos legales establecidos, Lantik solicitará controles de seguridad específicos y que podrán ser auditados.

8 Supervisión

.1 Lantik dispondrá de elementos de monitorización que permitan la auditoría de las actividades, las excepciones y eventos de seguridad dla entidad proveedora en función de las necesidades de la organización, disponiendo de estos registros durante el tiempo que se considere con el fin de servir como prueba forense y/o en la supervisión del control de accesos.

.2 Se supervisará el uso de los sistemas de información, por parte dla entidad proveedora y esta información se tratará periódicamente.

.3 Las actividades de administración y operación que pudieran ser realizadas por parte dla entidad proveedora de servicio sobre los sistemas de información de Lantik, serán registradas.

10. Control de acceso

Objetivos

- Impedir el acceso no autorizado a la información y los sistemas de información.
- Implementar seguridad en los accesos dla entidad proveedora por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de Lantik y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por la entidad proveedora en los sistemas.
- Concienciar a la entidad proveedora respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan portátiles e instalaciones remotas.
- Adquisición, desarrollo y mantenimiento de los sistemas de información

1. Requisitos de Lantik para el control de acceso

.1 La entidad proveedora únicamente tendrán acceso a aquellos recursos de red, aplicaciones e información que sean necesarios para el desempeño de las labores propias del servicio contratado. Los derechos de acceso a las mismas serán los mínimos posibles en función de dichas necesidades. Las reglas de control de accesos se establecerán de acuerdo a la “necesidad de saber”.

2. Gestión de acceso de usuario

.1 Todo proveedor, previa a la prestación y a la finalización del servicio en lantik, deberá solicitar el alta y baja de usuarios en base al procedimiento formal de registro y anulación de usuarios que concede y revoca el acceso a los sistemas de información.

.2 Todo cambio en la prestación del servicio que suponga cambio en las personas que participan en el mismo deberá ser notificada a la mayor brevedad a Lantik con el fin de realizar las bajas y altas correspondientes. Lantik se reserva el derecho de auditar periódicamente las asignaciones realizadas.

3. Responsabilidades del usuario

.1 Se requerirá a la entidad proveedora el uso de buenas prácticas de seguridad en la selección y uso de contraseñas sobre sus sistemas de información, sobre todo en aquellos que no dispongan de políticas automáticas de calidad de contraseña.

.2 Se requerirá a la entidad proveedora el puesto de trabajo despejado de papeles y de soportes de información si no se están utilizando y la ocultación de información de la pantalla del equipo si no se está delante.

4. Control de acceso a red

.1 Se proporcionará a la entidad proveedora acceso a los servicios de red requeridos para la prestación del servicio contratado.

.2 Las conexiones externas de una entidad proveedora a infraestructuras de Lantik, deberán ser previamente validadas. En función del análisis del riesgo de la conexión, se requerirán controles de seguridad auditables.

.3 Se prohíbe el acceso físico y lógico a los puertos de diagnóstico y de configuración de las infraestructuras de Lantik. En caso de requerirse por definición del servicio, se registrarán dichos accesos.

.4 En base a la arquitectura de red segregada, las conexiones a las mismas se realizarán en función de las necesidades concretas de conectividad para la prestación del servicio. Se prohíbe la configuración de rutas o accesos no validados previamente por Lantik.

5. Control de acceso a los sistemas operativos

.1 Para el equipamiento de usuario, el acceso a los sistemas operativos requerirá inicio de sesión válido sobre el dominio de Lantik si así lo exige el servicio. Para los servidores y equipamiento de comunicaciones se requerirá la asignación específica de funciones de administración. En los casos en los que lo exija el servicio.

.2 Todos los usuarios dispondrán de identificador único de usuario para su uso personal y exclusivo.

.3 Se prohíbe de manera explícita el uso de aplicaciones y/o utilidades que pudieran invalidar los controles de acceso y/o aplicación y las no asociadas a la prestación del servicio contratado.

.4 Sobre los sistemas de información sobre los que se identifiquen niveles de riesgo extraordinarios se utilizarán restricciones en los tiempos de conexión.

6. Control de acceso a las aplicaciones y a la información

.1 El acceso a la información será restringida en función a su necesidad de conocer para los servicios contratados a cada proveedor.

11. Adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivos

- Cumplir los controles de seguridad en el ciclo de vida de los sistemas de información.
- Cumplir las normas y procedimientos que se aplican durante el ciclo de vida de las aplicaciones y en la infraestructura de base en la cual se apoyan.
- Regular el uso de información confidencial.
- Garantizar el procesamiento correcto de las aplicaciones.
- Garantizar el uso correcto de la información en los distintos entornos de desarrollo, prueba y producción.
- Minimizar las vulnerabilidades técnicas.

1. Requisitos de seguridad de los sistemas de información

.1 Previa a la contratación y/o adquisición de nuevos servicios se realizará un análisis previo en relación a la seguridad de la información por parte de Lantik. Si se considera oportuno, se incluirán requerimientos específicos en esta materia junto a los requisitos funcionales.

2. Tratamiento correcto de las aplicaciones

.1 Se establecerá la validación de los datos de entrada en las aplicaciones desarrolladas con el fin de garantizar que los mismos son correctos y adecuados.

.2 Sobre las aplicaciones desarrolladas se establecerán controles de procesamiento interno que permitan la detección de cualquier modificación de la integridad de la información tanto por error como de manera intencionada.

.3 Se establecerán controles de seguridad que garanticen los mecanismos de comunicación entre procesos, la autenticación e integridad de los mensajes.

.4 Se establecerán controles para la validación de datos de salida de las aplicaciones que permitan garantizar que la información almacenada es correcta y adecuada.

.5 Se aplicara la sistemática de Desarrollo y Mantenimiento de aplicaciones existente en Lantik (procedimientos, instrucciones técnicas y formatos).

3. Controles criptográficos

.1 El cifrado de información seguirá los requerimientos establecidos por lantik para el cumplimiento de requisitos legales y de negocio, empleando algoritmo de cifrado fuerte que no padezca vulnerabilidades ni debilidades conocidas y utilizando una herramienta informática adecuada para la utilización del algoritmo y clave.

.2 Las claves criptográficas utilizadas por parte dla entidad proveedora estarán protegidas contra modificación, pérdida y destrucción. Se tendrá en cuenta la autenticidad de las claves públicas empleadas. El proceso de autenticación se llevará a cabo utilizando certificados de clave pública expedidos por una autoridad de certificación reconocida que contará con los controles y procedimientos adecuados para ofrecer el grado de confianza necesario.

4. Seguridad de los archivos del sistema

.1 Se utilizarán los procedimientos de los que se dispone en Lantik para la instalación y actualización de software en los entornos de producción.

.2 Se evitarán el uso de datos reales en el entorno de pruebas. En caso de recurrir a datos de este tipo, la entidad proveedora deberá disponer de la correspondiente validación por parte de Lantik y previa a su utilización en el entorno de pruebas se garantizará la disociación de dicha información. En todo caso la información utilizada para pruebas estarán en todo momento protegida y controlada.

.3 El acceso al código fuente de los programas y a los elementos relacionados con él (diseños, especificaciones, planes de verificación y validación) estarán estrictamente controlados por Lantik, para evitar cambios involuntarios o la introducción de funciones no autorizadas.

5. Seguridad en los procesos de desarrollo y soporte

.1 Previos a la introducción de nuevos sistemas o de cambios importantes en los ya existentes, la entidad proveedora seguirá el proceso de gestión de cambios establecido en Lantik

.2 Se evitarán las situaciones que permitan que se produzcan fugas de información. La entidad proveedora tendrá la obligación de notificar a Lantik a la mayor brevedad estas situaciones.

.3 El desarrollo realizado por la entidad proveedora será supervisado y controlado por Lantik en base a los requerimientos previamente establecidos en el correspondiente contrato de relación.

6. Gestión de las vulnerabilidades técnicas

.1 Las vulnerabilidades técnicas identificadas en los sistemas de información no serán explotadas por la entidad proveedora de servicios. Serán notificadas a la mayor brevedad a Lantik.

12. Gestión de incidentes de seguridad de la información

Objetivos

- Establecer canales de comunicación de eventos y debilidades relativos a la seguridad de la información.
- Gestionar los incidentes de seguridad.
- Aprender de los incidentes de seguridad.

1. Notificación de eventos y puntos débiles de la seguridad de la información

.1 La entidad proveedora estará obligado a notificar cualquier incidente de seguridad que se produzca en la prestación del servicio. Esta notificación deberá realizarse a la mayor brevedad a través del centro de atención al usuario (CAU). Se emplearán además los elementos de supervisión, alertas y vulnerabilidades de que se dispone para detectar incidentes de seguridad de la información.

.2 Cualquier punto débil, en relación a la seguridad de la información, deberá ser notificado a través del centro de atención al usuario (CAU). No se deberá intentar comprobar ningún punto débil de seguridad que se sospeche que exista.

2. Gestión de incidentes de seguridad de la información y mejoras

.1 Todos los incidentes de seguridad serán gestionados por Lantik y podrán requerir la colaboración dla entidad proveedora para su resolución.

.2 En base a la gestión anteriormente indicada se dispondrá de información que permita su explotación para el análisis y aprendizaje de las partes implicadas.

.3 Las evidencias recopiladas en la gestión de un incidente de seguridad podrán ser requeridas por el órgano judicial competente por lo que serán convenientemente almacenadas y custodiadas.

13. Gestión de la continuidad de Lantik

Objetivos

- Establecer las pautas de actuación a seguir para garantizar la continuidad de los procesos de negocio.
- Establecer las pautas a seguir para llevar a cabo la activación y desactivación del plan.

1. Aspectos de seguridad de la información en la gestión de la continuidad de Lantik

.1 Los planes de contingencia derivados del plan de continuidad de negocio, que permiten mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y tiempo requerido, pueden requerir la intervención de la entidad proveedora de servicio.

.2 El plan de continuidad de negocio y los planes de contingencia derivados serán probados y actualizados periódicamente para asegurar su efectividad. Se garantizará que todos los miembros de los equipos de recuperación, así como cualquier entidad proveedora afectada, conoce sus responsabilidades.

14. Cumplimiento

Objetivos

- Cumplir con las disposiciones legales, normativas y contractuales a fin de evitar sanciones administrativas a Lantik y/o al empleado, o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que la entidad proveedora cumplan con la política, normas y procedimientos de seguridad de Lantik.
- Revisar la seguridad dla entidad proveedora de Lantik periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información utilizados para la prestación.
- Optimizar la eficacia del proceso de auditoría sobre la entidad proveedora de servicio.

1. Cumplimiento de los requerimientos legales

.1 La entidad proveedora garantizará el cumplimiento de la normativa establecida en relación al uso de material sobre el que puedan existir derechos de propiedad intelectual.

.2 La entidad proveedora velará por la protección de los activos de Lantik frente a distintas amenazas, durante el tiempo y forma que se establezca en la relación contractual, en base a los requerimientos legales, reglamentarios y empresariales.

.3 La entidad proveedora garantizará el cumplimiento de los requerimientos establecidos por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y las medidas identificadas en el Real Decreto que la desarrolla. Del mismo modo, la entidad proveedora asignado como encargado de tratamiento de ficheros de Lantik con datos de carácter personal cumplirá los requerimientos establecidos por Lantik como propietario de dichos ficheros.

.4 La presente Normativa de Seguridad de la Información para entidades proveedoras así como la derivada de la misma constituyen elementos que previenen el uso indebido tanto de la información como de los recursos de tratamiento de la información.

2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

.1 La entidad proveedora se asegurará, dentro de su ámbito, del cumplimiento de las normativas establecidas en relación a la seguridad de la información. El resultado de las revisiones de cumplimiento y las acciones correctivas derivadas constituirán evidencias de gestión de la seguridad de la información en cada ámbito de responsabilidad, a considerar en las revisiones de la provisión.

.2 En función del servicio contratado y las necesidades de Lantik, se realizarán comprobaciones de cumplimiento técnico sobre los recursos de tratamiento de la información, en base a la normativa establecida en Lantik para la gestión de la seguridad de la información.

3. Consideración sobre la auditoría de los sistemas de información

.1 Las auditorías de cumplimiento serán previamente planificadas con el fin de evitar riesgos sobre los activos de Lantik y los servicios prestados.

.2 Tanto las herramientas de auditoría como los registros obtenidos en el proceso se mantendrán en entornos diferentes a los de desarrollo u operativos con el fin de evitar cualquier peligro o uso indebido. Si en la auditoría participa o la realiza enteramente un proveedor, se podrá considerar la evaluación del riesgo previo que esto suponga y el requerimiento de controles de seguridad específicos sobre la entidad proveedora.

15. Auditoría

A requerimiento de Lantik, se podrán realizar auditorías de cumplimiento sobre los puntos indicados, con el fin de determinar el grado de cumplimiento de la Normativa de Seguridad de la Información para entidades proveedoras y establecer acciones correctivas en su caso.

16. Documentos relacionados

Norma Interna NCS-1/1 Norma de Seguridad: Código de Conducta Informático para Entidades proveedoras

17. HISTORIAL DE REVISIONES

Revisión	Fecha	Modificaciones
00	02/05/11	Aprobación de la norma
01	21/09/18	• Se revisa y adapta el documento a la normativa reguladora en materia de Igualdad.