NORMATIVA DE SEGURIDAD PARA PROVEEDORES

Control de Versiones

Descripción	Autor	Revisión y Aprobación	Fecha	Versión
Documento Inicial	JBermejo	MHernandez	17/11/2022	**01**
Revisión Anual Corrección errata Cambio de título	JBermejo	MHernandez	25/09/2023	**02**
Revisión anual	ABarquilla	MHernandez	12/05/2025	**03**
Revisión anual	Abarquilla	Mhernandez	11/03/2026	**04**

ÍNDICE

1. OBJETIVO

La finalidad del presente documento es mitigar los riesgos asociados al acceso a los sistemas de información o recursos de Corporación Vectalia, en adelante, Vectalia, por parte de los proveedores de servicios.

El objetivo es proteger la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información y los sistemas de Vectalia y sus clientes.

Es responsabilidad del proveedor garantizar el conocimiento de las políticas de seguridad descritas en este documento a todos los empleados que desarrollen o puedan desarrollar trabajos para Vectalia, así como obtener su compromiso de cumplir y respetar dichas normas.

La política de seguridad de Corporación Vectalia se basa en las siguientes directrices fundamentales de seguridad, con base en los requisitos dispuestos en los estándares ISO/IEC 27001:2022 y el Esquema Nacional de Seguridad, asegurando así la calidad de los productos y servicios, así como la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas de información.

Con carácter general, los recursos tecnológicos deben ser considerados herramientas de producción al servicio del negocio de Vectalia, por lo que su uso debe estar destinado exclusivamente a fines profesionales y al cumplimiento de las prestaciones para las que fue contratado el empleado o profesional, debiendo utilizarse de forma adecuada a su naturaleza y a sus fines profesionales. Queda totalmente prohibido cualquier uso personal o privado de los recursos tecnológicos por los empleados o profesionales de la empresa, por lo que no se generará ninguna expectativa de intimidad o privacidad sobre estos ni sobre el uso que se haga de ellos por parte de los empleados o profesionales que presten servicios para Vectalia.

En todo caso, queda prohibida la utilización de los recursos tecnológicos que suponga la violación del contrato que rija la relación laboral o negocial. Dado que los recursos tecnológicos son herramientas de uso estrictamente profesional, los empleados y profesionales no deberán archivar, guardar, transmitir, distribuir, almacenar, descargar, instalar, copiar, visualizar o enviar contenidos o información personal, privada y/o ajena al desarrollo de la actividad profesional de Vectalia.

2. CONFIDENCIALIDAD DE LA INFORMACIÓN

El personal externo que tenga acceso a la información de Vectalia deberá considerar que esta es información confidencial.
Solo la información pública contenida en las áreas públicas de las páginas web de la organización podrá ser considerada como tal.

Todos los activos y/o la información a la que se haya tenido acceso, o que haya sido necesario elaborar para el desempeño de los servicios, deberán ser devueltos a la finalización de la relación contractual. Vectalia podrá solicitar al proveedor el borrado seguro de aquellos dispositivos que hayan tenido acceso a la información de la organización.

3. PROPIEDAD INTELECTUAL

El proveedor garantizará el cumplimiento de la normativa vigente en materia de Propiedad Intelectual: Real Decreto Legislativo 1/1996, Ley de Propiedad Intelectual, y sus modificaciones; Ley 21/2014, que traspone el contenido de las directivas europeas a la legislación española, y Ley 2/2019.

Queda completamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información de Vectalia.

Igualmente, todo uso, reproducción, cesión o comunicación pública de cualquier tipo de obra protegida por la propiedad intelectual queda estrictamente prohibido sin la debida autorización escrita. Solo se autoriza el uso producido, suministrado o autorizado por Vectalia.

4. POLÍTICA DE SEGURIDAD

4.1 Disposiciones generales

El proveedor proporcionará a Vectalia la relación de personas asociadas al servicio y deberá informar de cualquier cambio que se produzca durante la relación contractual.

Todo el personal asociado a los servicios prestados a Vectalia por el proveedor deberá cumplir con lo establecido en este documento, siendo responsabilidad del proveedor trasladar la presente política a sus empleados.

Vectalia podrá realizar auditorías o revisiones de cumplimiento a los proveedores cuando lo estime necesario, especialmente si el servicio prestado implica acceso a información crítica, confidencial o personal.

4.2 Responsabilidad de los usuarios

El proveedor deberá asegurar que el personal que realice trabajos para Vectalia respete los siguientes principios básicos:

- Dado que cada persona es responsable de la actividad desarrollada con su usuario, es imprescindible que mantenga bajo control sus credenciales.
- No se deberán usar las credenciales de otro usuario, aunque este le haya dado su autorización. En este caso, se debería solicitar a Vectalia un nuevo usuario, si fuera necesario.

4.3 Seguridad en la red

El acceso a los sistemas y servicios de red de la organización es otorgado solo a usuarios identificados y autenticados. La identificación se realizará con una cuenta de usuario asignada y la autenticación se realizará con una contraseña secreta.

Para todos los accesos externos vía VPN existe un doble factor de autenticación usando la tecnología de Forti, FortiToken, que genera un código de un solo uso mostrado en la aplicación móvil del usuario.

Los requisitos de autenticación de Vectalia son:

- Antes de tener acceso a cualquier sistema o recurso de la red, todos los usuarios deben ser identificados positivamente mediante su cuenta de usuario y su contraseña.
- La cuenta de usuario y la contraseña deben ser individuales.
- Todas las identidades digitales utilizadas por los proveedores deberán estar gestionadas bajo principios de mínimo privilegio, trazabilidad y revocación inmediata en caso de fin de contrato.
- La autenticación en sistemas por parte de usuarios y administradores será registrada en logs para actividades de auditoría y eventuales análisis forenses.

El acceso administrativo a la infraestructura virtual se realizará a través de los servidores bastión creados a tal efecto. El responsable del área de IT proporcionará la información necesaria a los proveedores afectados.

Todos los equipos conectados a las redes a través de las que circule la información deberán estar apropiadamente identificados, de modo que el tráfico de red pueda ser identificable.

Todos los accesos a los sistemas de información de Vectalia deberán estar protegidos, al menos, por un firewall que limite la capacidad de conexión.

Todo acceso remoto deberá realizarse mediante canales cifrados, con doble factor de autenticación y con capacidad de registro de logs para su trazabilidad.

El proveedor deberá garantizar que todos los relojes de los sistemas estén sincronizados entre sí y con la hora oficial.

El proveedor deberá declarar qué usuarios tendrán accesos privilegiados a sistemas de Vectalia y asegurar su control, auditoría y revocación inmediata si se cancela el contrato.

4.4 Uso de la información de autenticación secreta

Los empleados y contratistas que desarrollen actividades en la organización deben cumplir las siguientes reglas respecto al uso de la información de autenticación:

Las cuentas de usuario y las contraseñas son individuales e intransferibles.

- Está prohibido el uso de un nombre de usuario ajeno o facilitar la cuenta de usuario y su contraseña personal a un tercero.
- Queda absolutamente prohibido anotar las contraseñas de acceso en lugares visibles o públicos.
- Las credenciales (usuario y contraseña) no deben ser incluidas en aplicaciones donde puedan quedar expuestas (macros de hojas de cálculo, documentos o programas de tipo script).
- El usuario deberá cambiar la información de autenticación secreta cuando exista alguna indicación de su posible compromiso. Se recomienda no utilizar las mismas contraseñas para fines laborales y personales
- Las contraseñas deberán cumplir con las siguientes características en cuanto a complejidad:

o Incluir letras mayúsculas y minúsculas.
o Incluir al menos un número.
o Incluir al menos un carácter especial.

- La política de contraseñas de Vectalia establece:

o Intentos antes del bloqueo: 3.
o Tiempo de bloqueo: 30 minutos.
o Validez de la contraseña: 90 días.
o Nº de contraseñas recordadas: 24.

4.5 Seguridad de los dispositivos

Todos los dispositivos que accedan a información de Vectalia deberán cumplir con la política de seguridad establecida por Vectalia. El proveedor deberá tener en cuenta especialmente los siguientes puntos:

- El acceso a los sistemas debe realizarse de forma autenticada.
- Los equipos se mantendrán de acuerdo con las especificaciones del fabricante.
- Todo el software debe estar licenciado y dentro del ciclo de vida del producto concreto.

- Los dispositivos deberán estar actualizados a la última versión disponible en cuanto a parches de seguridad, tanto para el sistema operativo como para el software que contengan.
- Debe activarse el bloqueo de pantalla para que salte a los 15 minutos de inactividad. El desbloqueo deberá conllevar el uso de contraseñas, patrones de desbloqueo o mecanismos equivalentes que garanticen que el dispositivo no podrá ser utilizado por un usuario no autorizado.
- Todos los dispositivos deben contar, como mínimo, con un sistema de protección antimalware actualizado, tanto en su motor como en el fichero de firmas.
- Los dispositivos no dispondrán de ninguna herramienta que trate de descubrir información o realizar accesos no autorizados, tales como sniffers, herramientas de descubrimiento y escaneo de redes, herramientas de descubrimiento de contraseñas o similares. Si estas herramientas fueran necesarias para la realización de un trabajo concreto, deberán ser evaluadas y autorizadas por el responsable de seguridad de Vectalia.

Se velará especialmente por la seguridad de los equipos portátiles que contengan o accedan a información de Vectalia.

- Los equipos deberán transportarse debidamente protegidos frente a golpes.
- Se evitará la conexión a los sistemas de Vectalia desde redes Wi-Fi públicas o sin cifrado alguno.
- Se tomarán las precauciones necesarias para evitar la visión accidental, por parte de terceros, de cualquier contenido relacionado con Vectalia.

4.6 Seguridad Física

Todas las instalaciones desde las cuales el proveedor preste sus servicios a Vectalia deberán cumplir estos principios mínimos en cuanto a la seguridad física de sus instalaciones:

Todos los accesos deberían estar controlados, evitando accesos no autorizados a través de mecanismos de control, alarmas, cerraduras, cámaras de vigilancia, accesos biométricos, etc.

Siempre que sea posible, se recomienda establecer barreras físicas que requieran la identificación y autenticación (tarjetas, identificación biométrica, etc.).

Las instalaciones deberán contar con sistemas de detección de incendios. Es deseable que dichos sistemas sean automáticos o, al menos, que existan medidas de extinción manual y que todo el personal del proveedor las conozca.

Se deben establecer las condiciones ambientales requeridas por los fabricantes para el equipamiento informático (temperatura, aislamiento eléctrico, humedad, etc.).

Si se mantiene alguna copia de información responsabilidad de Vectalia, los sistemas que alberguen dicha información deberán contar al menos con las siguientes medidas de seguridad:

- Tener un control de acceso y registro de accesos a la ubicación física donde se encuentre.
- El acceso por parte del personal externo solo tendrá lugar en caso de necesidad, debidamente autorizado y bajo la supervisión del personal autorizado del proveedor.
- Deberían existir medidas de protección contra cortes eléctricos y/o picos de tensión que puedan afectar al contenido de dicha información.

4.7 Seguridad en el desarrollo

Todos los proveedores que realicen trabajos de desarrollo y/o pruebas de aplicaciones para Vectalia deberían adoptar las siguientes medidas:

- Se deberán utilizar técnicas de programación seguras tanto para los desarrollos nuevos como en las situaciones de reutilización de código donde es posible que no se conozcan las normas que se aplican al desarrollo o donde no sean coherentes con las buenas prácticas actuales.
- Los ambientes de desarrollo, prueba y producción estarán separados al menos de forma lógica.
- Durante las fases de desarrollo y pruebas se llevarán a cabo pruebas específicas de las funcionalidades de seguridad.
- Durante el proceso de desarrollo deberán realizarse pruebas específicas de seguridad (escaneo de vulnerabilidades, pruebas de penetración, validación de control de acceso, etc.) y documentarse sus resultados como parte del ciclo de vida del desarrollo.
- Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.
- Se deberían definir y documentar las reglas, entornos y procedimientos de transferencia hacia el entorno productivo.
- Todo el proceso de desarrollo de software externalizado será controlado y supervisado por Vectalia.
- Se deberían aplicar mecanismos de identificación, autentificación, control de acceso, auditoría e integridad durante todo el ciclo de vida del desarrollo.
- Si fuera necesario, se incorporarán medidas de autenticación y control de la integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.
- Los entornos de pruebas no usarán datos reales o en su defecto datos previamente disociados, garantizando las mismas medidas de seguridad que las existentes en los entornos de producción.
- Solo se transferirán a los entornos productivos las aplicaciones expresamente aprobadas por Vectalia.

- Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.
- El acceso al código fuente deberá estar limitado al personal adscrito al servicio proporcionado a Vectalia.

4.8 Seguridad en los sistemas

Cumplir con lo establecido en el punto de Seguridad de los dispositivos.

El proveedor deberá contar con una gestión de activos actualizada en la que se identifiquen los activos utilizados para la prestación del servicio a Vectalia.

Los activos utilizados para la prestación del servicio deberán contar, como mínimo, con las medidas de seguridad contenidas en el presente documento.

Todos los activos que se usen para prestar servicios a Vectalia deberán contar con un responsable encargado de asegurar que las medidas contempladas sean debidamente aplicadas.

Siempre que se utilice el correo electrónico en relación con el servicio prestado, el proveedor deberá respetar las siguientes premisas:

- No se permitirá la transmisión vía correo electrónico de información confidencial de Vectalia, salvo que la comunicación electrónica esté cifrada y el envío esté expresamente permitido.
- No se permitirá la transmisión vía correo electrónico de información que contenga datos de carácter personal de nivel alto, salvo que la comunicación electrónica esté cifrada y el envío esté expresamente permitido.

Siempre que para la prestación del servicio se haga uso del correo electrónico de Vectalia, se deberán respetar, al menos, los siguientes principios:

- Se considerará al correo electrónico como una herramienta más de trabajo proporcionada con el fin exclusivo del servicio contratado. Esta consideración facultará a Vectalia a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad de las personas y su derecho a la intimidad.
- El sistema de correo electrónico de Vectalia no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
- Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios).

4.9 Seguridad en la cadena de suministro de TIC

El proveedor deberá garantizar que los productos y servicios de TIC proporcionados a Vectalia, incluidos los que dependan de subcontratistas, cumplan con requisitos de seguridad acordes con esta normativa. Cualquier subcontratación deberá ser notificada previamente a Vectalia y autorizada por escrito.

4.10 Uso seguro de servicios en la nube

El proveedor se compromete a garantizar la seguridad de la información de Vectalia durante todo el ciclo de vida del servicio en la nube. Antes de la adquisición del servicio, el proveedor deberá proporcionar información clara y verificable sobre sus controles de seguridad, cumplimiento normativo, ubicación de los datos y subprocesadores utilizados.

Durante el uso y la gestión del servicio, el proveedor deberá aplicar medidas de protección adecuadas, incluyendo, entre otras, las siguientes: control de acceso, cifrado de datos en tránsito y en reposo, segregación de datos, monitoreo continuo, gestión de vulnerabilidades y respaldo de la información. Asimismo, el proveedor deberá garantizar que la información de la organización no sea accedida, procesada ni divulgada sin autorización previa y documentada.

Al finalizar el servicio, el proveedor deberá asegurar la devolución íntegra de la información y la eliminación segura de todos los datos almacenados, incluidas las copias de seguridad, conforme a las instrucciones de la organización y en cumplimiento de la normativa vigente. La organización se reserva el derecho de auditar o solicitar evidencias del cumplimiento de estas obligaciones en cualquier momento.

4.11 Terminación y eliminación de la Información

El proveedor se compromete a garantizar, al término de la relación contractual, la revocación inmediata y segura de todos los accesos otorgados a sistemas, aplicaciones, redes e instalaciones de la organización. Asimismo, deberá eliminar de manera segura y permanente toda la información confidencial, los datos personales o cualquier otro activo informacional perteneciente a la organización, incluidas las copias de respaldo y los soportes electrónicos o físicos, salvo que exista obligación legal de conservación. La eliminación deberá realizarse utilizando métodos que impidan su recuperación y deberá quedar documentada y disponible para su verificación por parte de la organización, si esta lo requiere.

4.12 Uso de Productos TIC Certificados

Se recomienda que el proveedor utilice preferentemente productos de tecnologías de la información y las comunicaciones (TIC) que estén incluidos en el Catálogo de Productos de Seguridad TIC (CPSTIC), publicado por el Centro Criptológico Nacional (CNN-CERT), en aquellos servicios, sistemas o infraestructuras

relacionados con la prestación del servicio contratado y que estén sujetos al cumplimiento del Esquema Nacional de Seguridad (ENS).

En caso de emplearse productos no incluidos en el CPSTIC, se sugiere que el proveedor documente adecuadamente su elección, incluyendo una evaluación de riesgos y medidas compensatorias, y que consulte con Vectalia para validar su idoneidad en el contexto del servicio.

5. CONTINUIDAD Y CAPACIDAD

Los proveedores de Vectalia deberán contar con planes de continuidad para que en caso de contingencia el servicio pueda continuar prestándose sin ver mermada su calidad y seguridad.

Los proveedores deberán contar con planes de continuidad, testados al menos de forma anual, que sirvan para recuperar el servicio en el plazo acordado en los contratos de servicios establecidos entre ambas partes.

6. GESTIÓN DE CAMBIOS

Los proveedores deberán contar con una gestión de cambios que garantice que todos los cambios en la infraestructura con la que se presten los servicios a Vectalia estén controlados y autorizados.

Los nuevos componentes incluidos en la infraestructura IT que presta servicio a Vectalia, deberán ser verificados y asegurar el cumplimiento de su propósito.

Se tratará de minimizar los cambios sobre los componentes críticos, ejecutando aquellos considerados como imprescindibles.

El proveedor analizará las vulnerabilidades técnicas sobre los activos que proveen servicio a Vectalia, informándole de las mismas con el objetivo de gestionarlas en conjunto.

7. COMUNICACIÓN DE INCIDENTES DE SEGURIDAD

Toda incidencia en materia de seguridad deberá comunicarse, siguiendo el procedimiento establecido. Dicha notificación será realizada a través de correo electrónico a incidencias@vectalia.es.

Una vez recibida el responsable de Seguridad será el encargado de darle seguimiento, completar las notificaciones establecidas en el procedimiento correspondiente, establecer las acciones para su corrección y comunicar al usuario la resolución o estado de esta.

Esta normativa será revisada como mínimo una vez al año, o siempre que se introduzcan cambios significativos en el entorno tecnológico o normativo. Los cambios realizados serán divulgados a las entidades proveedores de servicio que les aplique utilizando los medios que se consideren oportunos.

Es responsabilidad de cada organización garantizar la lectura y conocimiento de dichas políticas a su personal.