**POLITICA DE SEGURIDAD EN EL PROCESO DE DESARROLLO DE SOFTWARE**

**I.- DEFINICIONES ESTRATÉGICAS**

**a.- Objetivo general**

La empresa, a través de su [Comité de Riesgos y Seguridad de la Información], presenta en este documento la Política de Desarrollo de Software que establece la [Unidad TIC] cuyo objetivo es definir los procedimientos para desarrollar, evaluar, actualizar y poner en producción sistemas seguros que incluyan herramientas para control de acceso, control de errores y protección de los datos administrados por la empresa, en términos de seguridad de la información y a mantener la continuidad de las operaciones.

**b.- Objetivos específicos**

* Identificar los requerimientos de seguridad de cada una de las aplicaciones.
* Identificar toda la información relacionada con las aplicaciones (usuarios y restricciones de acceso, interoperabilidad, reglas de respaldo, disponibilidad y ventanas de trabajo entro otros).
* Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información en la Subsecretaría del Interior.
* Establecer los niveles de acceso apropiados a la información institucional, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

**c.- Consideraciones generales**

Desde las primeras etapas del proceso de Ingeniería de Software deben considerarse aspectos relativos a la seguridad de las aplicaciones.

Durante la etapa de análisis deben identificarse tanto los requisitos de seguridad como su respectiva validación.

En la etapa de Diseño deberán diseñarse los controles necesarios para satisfacer los requisitos identificados anteriormente.

En la etapa de Implementación deben implementarse los controles de seguridad además de aplicarse los controles relativos al proceso de desarrollo de software, aquellos controles que deban estar en la aplicación, como por ejemplo validaciones a realizarse en el software, encriptado, etc.

En fase de Verificación se debe verificar adecuadamente que los requisitos de seguridad de la aplicación se cumplen.

**d.- Alcance**

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la [Empresa XXX]. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de la [Empresa XXX], establecidos en el documento institucional denominado Definiciones Estratégicas o equivalente, cubriendo a toda la organización independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

**e.- Roles y Responsabilidades**

Las responsabilidades se encuentran definidas en la política de la organización de la seguridad de la información.

**f.- Vigencia y Actualización**

La Política se considera vigente desde la fecha de su aprobación por parte de la autoridad, documento que será revisado y actualizado cada dos años o cuando el Comité de Riesgos y Seguridad de la Información lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de la [Empresa XXX].

La Política deberá ser revisada por el Comité de Seguridad de la Información. No obstante, aquello, la [Unidad responsable de Ciberseguridad] promoverá la revisión permanente de esta Política y generará las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del SGSI.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

* Cambios en las leyes o reglamentos que afecten a la [Empresa XXX].
* Incorporación o modificaciones relevantes de procesos críticos de la [Empresa XXX].
* Cambios significativos al soporte tecnológico.
* Modificaciones en la estructura de la organización.
* Cambios significativos en los niveles de riesgo a que se expone la información.
* Cambios relevantes en las Definiciones Estratégicas.
* Ajustes necesarios producto de Estados de Excepción Constitucional.
* Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a la Política de General de Seguridad de la Información deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

**g.- Revisión del cumplimiento**

El Comité de Riesgos y Seguridad de la Información, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

**h.- Control de documentos**

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información (SGSI) deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

* Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
* Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de Riesgos y Seguridad, incorporando Tabla en Capitulo final en cada documento.
* Se deberá controlar el uso no intencionado de documentos obsoletos.
* En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

**i.- Difusión**

El mecanismo de difusión de la Política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el Comité de Riesgos y Seguridad de la Información estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

**II.- POLÍTICA DE SEGURIDAD EN EL PROCESO DE DESARROLLO DE SOFTWARE**

**a.- Descripción al proceso.**

La empresa desarrollará y mantendrá sus sistemas teniendo como prioridad el cumplimiento oportuno de los requerimientos de sus clientes (internos y externos) asegurando a su vez, tanto la calidad como la continuidad de las operaciones. Toda solicitud de modificación o de diseño de un nuevo sistema o programa computacional deberá estar debidamente justificada y será evaluada, en cuanto funcionalidad y seguridad, antes de ser aceptada. Quien presenta un requerimiento, deberá hacerlo con suficiente antelación teniendo en consideración tanto el tiempo requerido para su evaluación y ejecución, así como el impacto o efectos que su aplicación tendrá en los procesos de negocios y objetivos estratégicos.

La [Unidad TIC] será la responsable de validar y administrar los requerimientos que provengan de las distintas áreas de la empresa en materia de desarrollo de sistemas informáticos. Lo mismo aplicará para la adquisición de nuevos programas y sistemas de procesamiento de información. Consecuentemente con lo anterior, todas las soluciones de software, independientemente de su origen, serán visadas por la [Unidad TIC], desde las perspectivas de desarrollo de sistemas (funcionalidad, QA), de explotación de sistemas (plataforma, rendimientos, performance, pruebas de demandas altas de transacciones) y de ciberseguridad, antes de ponerlos en uso oficial o producción.

Los sistemas que se adquieran, modifiquen o que se desarrollen, deberán incluir manejo de errores, lo que se deberá verificar antes de comenzar su uso, a través de pruebas exhaustivas de seguridad, control de acceso y funcionalidades, las que serán realizadas tanto por personal de la [Unidad TIC] como por los usuarios representativos de la organización o dueños de la información y encargados del proceso.

Será responsabilidad de cada Unidad, determinar y justificar en términos de costo/beneficio las necesidades de automatización o modificaciones a los sistemas para mejorar su gestión, optimizar los procesos. No obstante, lo anterior, basado en las inquietudes recogidas, la [Unidad TIC] podrá establecer recomendaciones de mejora o la inclusión de nuevas soluciones de software que serán sometidas a evaluación del Directorio o Gerencia pertinente para ser parte de la cartera de iniciativas a desarrollar en el Plan de trabajo de la empresa.

**Aceptación y evaluación de requerimientos.**

Todos los requerimientos serán presentados formalmente y serán evaluados por la [Unidad TIC] en términos de su justificación, beneficios, costos y de su impacto en la seguridad considerando para esto último las exigencias de protección de datos. Los resultados de la evaluación serán revisados por las partes interesadas de tal manera de priorizar y de asignar los recursos que cada requerimiento amerite. En caso de no haber acuerdos en los cronogramas de trabajo, se expondrá situación al Directorio o Gerencia pertinente para su resolución.

**Lenguajes y herramientas de desarrollo.**

Los Sitios o Sistemas utilizarán lenguajes y herramientas de desarrollo estándar de mercado de tal manera de asegurar que los sistemas computacionales puedan ser adecuadamente mantenidos o actualizados según corresponda, teniendo presente que éstos evolucionan en el tiempo corrigiendo errores, dando de baja funciones e incorporando otras nuevas. Las herramientas que se utilicen serán estrictamente controladas y se usarán bajo autorización de la [Unidad TIC] cumpliendo con los requisitos de licenciamiento que corresponda.

**Propiedad de las aplicaciones y sistemas (código fuente).**

Todos los sistemas y soluciones desarrolladas por y para la empresa serán de propiedad exclusiva de la empresa y no podrán ser utilizados o facilitados a terceros sin autorización expresa de la [Unidad TIC] y la adecuada fundamentación técnica, económica y legal/contractual.

En el caso de paquetes desarrollados por terceros, se procurará adquirir los paquetes junto con sus programas fuente y si esto no fuera factible, se asegurará el mantenimiento y soporte a través de contratos que garanticen la disponibilidad de los programas fuente en caso de cese de funciones del proveedor o bien se disponga del modelo de datos y su comprensión para continuidad de operación después de vencido el contrato. Se velará siempre porque los datos creados con dichas herramientas son de propiedad de la empresa, y se exigirá acceso irrestricto a las auditorías y trazas de funcionalidad y seguridad.

**Documentación.**

Será obligatorio para quienes estén a cargo del desarrollo o mantenimiento de sistemas, el diseñar documentación adecuada y aclaratoria respecto de la lógica y de las técnicas utilizadas, de tal manera que permita su comprensión por parte de terceros. Corresponderá a la [Unidad TIC] establecer estándares de calidad, seguridad y contenido para la documentación requerida.

**Custodia de programas.**

La [Unidad TIC] establecerá responsabilidades individuales y procedimientos que permitan custodiar y proteger los programas fuente de tal manera de controlar las versiones y los cambios aplicados al código fuente. Junto con lo anterior, en los ambientes productivos se protegerá a los programas ejecutables y software base, de tal manera que no sean intervenidos o alterados sin contar con las aprobaciones necesarias.

**Puesta en marcha de aplicaciones.**

Todos los cambios y puesta en marcha (paso a producción) de nuevos programas o sistemas estarán sujetos a una planificación y acuerdos con el área requirente de manera de no interrumpir ni poner en riesgo los procesos críticos del negocio.

Dado esto se considerarán los niveles de riesgo asociados con el cambio adoptando medidas de resguardo que permitan una eventual vuelta atrás en el caso que se obtengan resultados o efectos diferentes de los esperados.

**Cambios mayores.**

En los casos en que los cambios o incorporación de sistemas tengan un alto impacto en las operaciones o en los datos del negocio, se procurará establecer períodos de marcha blanca o planes piloto aplicados sobre una muestra representativa, antes de su puesta en marcha definitiva.

**Seguridad de los ambientes de desarrollo.**

Los equipos y herramientas que se utilicen para del desarrollo o mantenimiento de los sistemas estarán protegidos con acceso exclusivo para el personal que cumple las funciones de mantener o diseñar nuevos sistemas.

Se procurará proveer herramientas e interfaces que ayuden a los equipos de desarrollo en la aplicación de técnicas de desarrollo seguro de manera de identificar los problemas lo más tempranamente posible.

**Seguridad de aplicaciones.**

Las aplicaciones se desarrollarán utilizando técnicas y mecanismos de seguridad que permitan reducir o controlar los riesgos de acceso no autorizado, registrar el detalle y autoría de operaciones sensibles sobre los datos y de prevenir ataques o intervenciones de terceros.

En los casos que corresponda, una vez que las aplicaciones estén en sus distintas fases: diseño, testing funcional/ testing seguridad, QA funcional / QA seguridad, y producción, teniendo en especial consideración para aquellas que se exponen fuera de la red corporativa, es decir, son expuestas a internet, la [Unidad TIC] realizará revisiones periódicas de vulnerabilidades, test de penetración, ethical hacking para descubrir eventuales debilidades y problemas que pudieran afectar al aplicativo mismo o a la plataforma que las contiene o a las herramientas de desarrollo utilizadas.

**b.- Ambientes en el proceso de Desarrollo**

Se procurará contar con tres ambientes completos para el ciclo de ingeniería de software. Si el desarrollo es externalizado estos requerimientos caerán en el proveedor y deberán ser supervigilados por la [Unidad TIC]. Estos ambientes serán:

**Desarrollo**

* Es el ambiente propio de los desarrolladores.
* El ambiente debe ser accedido desde la red interna del Ministerio, prohibiendo su acceso desde VPN u otros medios.
* El desarrollador es el responsable del mantenimiento del ambiente.
* Se debe utilizar productos y entornos equivalentes a los empleados en producción, de manera de crear ambientes de trabajo equivalentes al de producción. Sólo en casos debidamente justificados y que son evaluado por la [Unidad TIC], el ambiente de desarrollo podrá no ser semejante al de producción. La regla general es que el ambiente de desarrollo es igual que el ambiente de testing, el que a su vez es igual al ambiente de producción. Se admiten diferencias en capacidad de los equipamientos y tamaños de las bases de datos, pues se debe equilibrar la necesidad legítima de contar con entornos iguales contra los recursos tecnológicos y económicos existentes, estando abierta la posibilidad de la utilización de entornos en la nube con los debidos resguardos de seguridad para el tratamiento de información confidencial, interna o de terceras partes.
* Los desarrolladores deben contar con el máximo de información posible que les ayude a depurar y tomar conocimiento de los errores que surgen de la puesta en marcha de sus desarrollos en cada una de las fases, incluyendo el nivel de producción. Los encargados de sistemas para cada una de las fases de desarrollo deberán acceso a la información de LOGs que sean pertinentes a los desarrolladores con motivo de coadyuvar al proceso de depuración de errores, sobre todo cuando un sistema está en producción y su utilización es crítica.

**Pruebas**

Es el ambiente en el cual se realizan las pruebas de caja negra[[1]](#footnote-1) o caja gris a las aplicaciones.

* Deberá replicar productos y configuración respecto del ambiente de producción.
* La administración de este ambiente estará a cargo de la [Unidad TIC].
* El personal del desarrollo no deberá acceder a la administración de este ambiente, pero sí podrá participar en las pruebas a realizar en el mismo.
* Este ambiente es exclusivo de Pruebas y no deberá en ningún momento, salvo las excepciones acordadas en conjunto por los responsables de seguridad, los responsables de plataforma y los desarrolladores, apuntar a datos de producción.
* Los datos de prueba, que requieran realizarse con externos, deberán ser anonimizados.
* Las Bases de datos de prueba deberán eliminarse una vez terminada la etapa de pruebas.

**Producción**

Es el ambiente operativo.

* La administración de este ambiente deberá estar a cargo de la [Unidad TIC].
* En este ambiente de trabajo se implementan medidas de seguridad que persiguen garantizar la protección del software de sistemas, los datos institucionales y los datos de los usuarios del sistema ya sean internos o externos.
* El personal del desarrollo no deberá acceder a la administración de este ambiente, pero si debe tener acceso a toda información relevante que ayude a la detección de errores para acelerar el proceso de resolución. En esta última condición caen todos los LOGS que puedan ayudar a los equipos de desarrollo a entender los problemas que la aplicación pueda estar presentando tanto desde la óptica de funcionalidad como de seguridad.
* No se deberán realizar pruebas que modifiquen datos en este ambiente.

**c.- Control de Acceso a aplicaciones en producción**

Todos los sitios o sistemas que no sean de libre acceso deberán contar con control de acceso basado en roles y perfiles de usuario, los cuales serán administrados por el usuario encargado del sistema que pertenece a la Unidad “dueña” del sistema. Los accesos a las Bases de Datos a través de las aplicaciones son establecidos por medio de conectores, de modo que los usuarios de los sistemas no están autorizados para acceder a las Bases de Datos.

**d.- Controles Criptográficos**

Se utilizarán sistemas y técnicas criptográficas para el acceso y almacenamiento de las claves de usuarios, las bases de datos del sistema y para la transmisión de datos de la empresa.

Todo sitio o sistema web deberá encriptar todas las comunicaciones entre el cliente y el servidor. Es obligatorio utilizar HTTPS en vez de HTTP, utilizando certificados válidamente emitidos por compañías debidamente acreditadas en el país y de reputación reconocida en el mercado que cuente con las debidas certificaciones normativas y legales, y en ningún caso se autorizará la utilización de certificados autogenerados, que si bien son utilizables para entonos experimentales y pruebas de concepto, no son admisibles para un entono de producción.

**e.- Seguridad de los Archivos del Sistema**

Se garantizará que los accesos a los archivos de sistemas, contenidos en los Servidores administrados por la [Unidad TIC], serán protegidos de accesos no autorizados. Todo esto teniendo en consideración:

* La protección de los archivos en el disco duro.
* Que ningún programa podrá acceder a archivos y/o carpetas en los sistemas que no sean de su propiedad.
* Que los archivos propios de cada aplicación deberán guardarse en lugares predefinidos. En el caso de las aplicaciones de escritorio, deberá acordarse un lugar donde el sistema operativo en el cual se corre la aplicación le provea al usuario la capacidad de guardar archivos de aplicaciones, evitando la necesidad de derechos especiales para la ejecución de estos programas.
* Que en el caso de las aplicaciones alojadas en servidores deberá acordarse un lugar donde la aplicación deberá acceder. A lo cual, deberá mantenerse el debido aislamiento de otras aplicaciones alojadas en un mismo Servidor.

**f.- Control de Acceso a las Bibliotecas de Programas Fuentes**

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán medidas y controles que aseguren la custodia de éstos, para lo cual se deberán cumplir las siguientes funciones:

* Proveer a la [Unidad TIC] los códigos fuentes solicitados para su modificación, manteniendo en todo momento la correlación código fuente / ejecutable vía “subversion” o similar.
* Llevar un registro actualizado de todo el código fuente en uso, indicando nombre del programa, programador, analista responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en desarrollo, pruebas, o producción).
* Verificar que el responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario.
* Administrar las distintas versiones de una aplicación.
* Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
* Prohibir la guarda de programas o código fuente histórico (que no sea correspondiente a los programas operativos) en el ambiente de producción.
* Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.

**g.- Control del Software Operativo**

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

* Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
* El responsable del Desarrollo deberá:
  + Coordinar la implantación de modificaciones o nuevos programas en el ambiente de Producción.
  + Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
  + Solicitar la Instalación de las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del dueño de la información y del grupo encargado de la verificación.

**h.- Protección de los Datos de Producción**

Se prohíbe el uso de base de datos operativas (de producción) para la realización de pruebas y/o exportación de modelos y datos con externos.

**i.- Control de Cambios a Datos de Producción**

La [Unidad TIC] mantendrá Procedimiento de Control del software operacional para el registro de los cambios.

**j.- Canales Ocultos y Código Malicioso**

Para evitar la existencia código malicioso en los sistemas, se deberán establecer normas y procedimientos que incluyan:

* Adquirir programas a proveedores acreditados o productos ya evaluados.
* Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
* Controlar el acceso y las modificaciones al código instalado.
* Utilizar herramientas para la protección contra la infección del software con código malicioso.
* Monitorear y analizar el tráfico de red de los aplicativos para detectar anomalías, en lo posible de manera automatizada mediante tecnologías SIEM, SOAR, IDS/IPS e IA.

**k.- Auditoría y Trazabilidad.**

Todo sistema deberá tener un registro de auditoría, trazas (logs) y monitoreo centralizado que provea herramientas para su administración, y a su vez la capacidad para enviar logs a otros sistemas de ciberseguridad que coadyuven a la identificación de anomalías.

La información de auditoría deberá presentarse mediante un aplicativo de usuario final de forma que sea fácilmente legible y entendible, pudiéndose realizar reportes y estadísticas de uso de forma sencilla y precisa.

Se deberá contar con un registro de los datos que se modifican, datos viejos y datos nuevos, y marcas de tiempo (timestamp). Esta actividad podrá ser realizada por la aplicación y/o por propia base de datos.

Como se mencionó anteriormente se deberá registrar y auditar las actividades relativas a la administración de claves.

**l.- Validación de Datos de Entrada y Control de errores**

Los datos de entrada a los sistemas serán validados para asegurar que son correctos y apropiados y que no facilitan posibles fallas o caídas de los sistemas que los soportan.

Para esto se deberán tener en cuenta las siguientes directrices:

* Comprobar que los datos ingresados corresponden al tipo de datos solicitados.
* Comprobar que los datos estén en el formato especificado.
* Comprobar que el tamaño de los datos de entrada no supere el tamaño total del campo.
* Utilizar listas de selección de valores predeterminados, para disminuir ingreso errado de datos.
* Comprobar límites inferiores y superiores.
* Comprobar que los datos obligatorios sean ingresados.
* Usar dígitos de verificación cuando corresponda.
* Los campos de contraseñas no deberán ser legibles.
* Las contraseñas de ingreso o autorización a definir e ingresar, deberán ser validadas respecto a las políticas de contraseñas definidas (largo, tipos de caracteres requeridos, antigüedad e historial), guardando la integración con el sistema de autenticación.
* Complementariamente cuando exista posibilidad de ataques de fuerza bruta o automatizados deberán implementarse controles del tipo captcha[[2]](#footnote-2) o similares.

Respecto al control de errores, en las aplicaciones se deberá contemplar lo siguiente:

* El correspondiente y aclaratorio mensaje de error, cuando los datos ingresados no sean los correctos, en relación con las funciones de validación establecidas. Estos errores serán registrados o trazados (loggeados) y analizados para indagar las causas que los están provocando: intencionales o no intencionales, generándose notificaciones al equipo de seguridad de la información cuando corresponda.
* Los programas deberán permitir concluir las transacciones correctamente, aun después de fallas. Esto considera privilegiar la integridad de los registros de información.

Por otra parte, para análisis de errores y calidad del software se llevarán a cabo las siguientes acciones:

* Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.
* Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.
* Se deberán revisar con “usuario dueño del sistema” las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

**m.- Utilización de estándares.**

Todo desarrollo de software estará sujeto a los estándares que defina la [Unidad TIC] y que son adicionales a los estándares ISO y los estándares de la industria que guíen la utilización de metodologías, paradigmas, IDE’s, Bibliotecas, patrones y otros, con enfoque de seguridad, resiliencia, interoperabilidad, tolerancia a altas demandas, entre otros.

Estos estándares, en específico se refieren principalmente a los siguientes aspectos:

* Lenguajes de Programación que se permiten.
* Herramientas de apoyo al desarrollo de sistemas.
* Programación de SQL y accesos a Bases de datos de modo que aplicaciones sean portables y seguras.
* Reutilización de código (Rutinas y Bibliotecas institucionales) validadas por seguridad.
* Conexiones a Bases de Datos.

**III.- ADQUISICIÓN DE PAQUETES DE SOFTWARE**

En el caso que se opte por la adquisición de soluciones o paquetes de software externo, será requisito la evaluación técnica, financiera y legal/contractual del proveedor y la evaluación funcional y tecnológica de la solución ofrecida por parte de la [Unidad TIC] y Unidad que lo requiere.

La instalación y el uso de dichos paquetes estarán sujetos a los acuerdos de licencia y en los contratos se consignarán garantías de calidad, soporte y mantenimiento que respalden a la organización en el caso que el software no cumpla en alguna forma con los requisitos del negocio, los que no obstante se validarán exhaustivamente antes de decidir la compra.

Como se indica en párrafos anteriores, los contratos también deberán considerar las condiciones de resguardo en los casos de disolución o cese de actividades por parte del proveedor o de la eventual cesación de los servicios de soporte y mantenimiento. en especial si el servicio se presta a través de infraestructura en la nube.

**IV.- PROVEEDORES EXTERNOS DE DESARROLLO**

En los casos en que se acuerde el desarrollo de aplicaciones por parte de un proveedor externo, éste deberá aceptar y aplicar las políticas de Seguridad que la organización haya establecido para los procesos de desarrollo, incluido los compromisos de confidencialidad, los derechos de propiedad intelectual, las condiciones de soporte y mantenimiento y las condiciones relativas al cese de sus actividades o traspaso de sus servicios a terceros, en caso de que se permita.

Para la realización de las pruebas de software, los proveedores de desarrollo deberán proveer datos ficticios o anonimizados, evitando la utilización de datos reales.

**V.- DESARROLLOS DE USUARIOS**

En caso de que personal, ajeno a la [Unidad TIC], elabore soluciones de software de apoyo a sus gestiones, en que manipulen datos de la empresa, deberán aplicar estas políticas de seguridad y de respaldos sobre la información. Estos solo podrán operar si cuenta con la debida autorización de la [Unidad TIC] y la jefatura directa del usuario.

Será responsabilidad de cada unidad organizacional asegurar que se cumpla con las políticas de seguridad, en lo que se refiere a resguardo del código fuente, acceso restringido y respaldo de datos. Además, deberán cumplir con el requisito de informar a la [Unidad TIC], de traspasar una copia y manual de funcionamiento del software, así como de las modificaciones o actualizaciones de este.

Cabe indicar que en todos los casos la propiedad intelectual por el desarrollo de soluciones de parte de usuarios, en el desempeño de sus cargos, pertenecerá al la empresa ( Art° 88 Ley 17.336 sobre Derecho de Autor).

1. https://es.wikipedia.org/wiki/Caja\_negra\_(sistemas) [↑](#footnote-ref-1)
2. https://es.wikipedia.org/wiki/Captcha [↑](#footnote-ref-2)