— POLÍTICA  
  
POLÍTICA DE SEGURIDAD DE  
  
| PO-SS1-014  
  
CENABAST  
  
ADQUISICIÓN, DESARROLLO Y  
MANTENIMIENTO DE LOS SISTEMAS DE  
  
INFORMACIÓN  
  
POLÍTICA DE SEGURIDAD DE  
  
ADQUISICIÓN, DESARROLLO Y  
MANTENIMIENTO DE LOS  
  
SISTEMAS DE INFORMACIÓN  
  
Controles IS027001:2013  
  
A.14.1.1 A.14.2.2 A.14.2.6  
A.14.1.2 A.14.2.3 A.14.2.7  
A.14.1.3 A.14.2.4 A.14.2.8  
A.14.2.1 A.14.2.5 A.14.2.9  
  
Firma de los responsaples:  
  
Elaborado por:

Z -»P0LÍTICA “| PO-SsI-014  
CENABAST | POLÍTICA DE SEGURIDAD DE  
ADQUISICIÓN, DESARROLLO Y  
MANTENIMIENTO DE LOS SISTEMAS DE  
INFORMACIÓN  
  
Indice .  
1. Objetivo ....................eereermsenan eoe nn oee De eee eoe eoe re eee eee 3  
7[1 ( A T 3  
3. Rolesy Responsabilidades......................eceerereee DD D D D 3  
4. Política ..................eee eee nn nn nnc eeec eee oe eeec re re eee eeeccc 4  
4.1 Requisitos de seguridad de los sistemas de información................1.seemenenec re 4  
4.1.1 Análisis y especificación de los requisitos de seguridad ..................—....eree.ecereereeeen. 4  
  
4.1.2 Protección de servicios de aplicación en redes públicas.  
  
4.2 Seguridad en los procesos de desarrollo y soporte.....................==e.e.eneee eee 5  
4.2.1 Política de desarrollo seguro de software.........................es0erie00 e D 6  
  
4.2.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo....6  
  
4.2.3 Restricciones a los cambios en los paquetes de software .....................—..rerere.eree00... 6  
4.2.4 Uso de principios de ingeniería en protección de sistemas ...................emrevererererereereees 7  
4.2.5 Seguridad de entornos de desarrollo .....................e.e.eienei e De 7  
4.2.6 Externalización del desarrollo de software .................ee.ererereieer D 8  
  
4.2.7 Pruebas de funcionalidad durante el desarrollo de los sistemas..  
  
4.2.8 Pruebas de aceptación .................e.e.ereriee e eee eee 9  
5. Difusión de la Política .......................e.ererene eee e eee ee ee eeec eee eee 9  
6. Revisión de la Política .......................e.e.eeeeeee eee ee D eee eeec eee eee 9  
7. Glosario de términos .............e.0se00remeseereeee e Dr eee ee eee eee 9  
8. Control de Cambios. ......................eeeeeieeeree DD e eee re eee eee eee 10

s R Y rosso  
CENABAST POLÍTICA DE SEGURIDAD DE . REVSÓN -| 480  
  
ADQUISICIÓN, DESARROLLO Y  
  
MANTENIMIENTO DE LOS SISTEMAS DE — "\*?  
  
INFORMACIÓN — PÁGINAS  
  
1. Objetivo  
  
Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo  
de vida de desarrollo de los sistemas de información de CENABAST, aplicando los  
resguardos que permitan asegurar la seguridad de los sistemas de información y de  
los procesos de construcción, mantención o adquisición de éstos.  
  
2. Alcance  
  
Esta Política se aplica a todos los sistemas informáticos que dan soporte a los  
productos estratégicos de CENABAST, tantos desarrollos propios o de terceros, y a  
todos los sistemas operativos y/o software de base que integren cualquiera de los  
ambientes administrados por la institución en donde residan los desarrollos  
mencionados.  
  
3. Roles y Responsabilidades  
Encargado de Seguridad de la Información:  
  
e Definir los controles a ser implementados en los sistemas desarrollados  
internamente o por terceros, en función de una evaluación previa de riesgos.  
  
e Definir en función a la criticidad de la información, los requerimientos de  
protección mediante métodos criptográficos.  
  
e — Verificar el cumplimiento de las definiciones establecidas sobre los controles y  
las medidas de seguridad a ser incorporadas a los sistemas.  
  
Jefatura Unidad Tecnologías de la Información:  
  
e Definir y dictar las políticas, estándares en tecnologías, seguridad de la  
información (integridad y confidencialidad) y su soporte tecnológico, velando  
por el cumplimiento de la normativa legal.  
  
e Revisar, aprobar (o rechazar) procesos y controles tendientes a mitigar,  
eliminar, o transferir los riesgos relacionados con la construcción, mantención  
y adquisición de sistemas de información, y según corresponda, definir  
procedimientos para ello.  
  
e Verificar el cumplimiento de los procedimientos y controles de seguridad  
establecidos para la construcción, mantención, y adquisición de sistemas de  
información.

= — AN s  
C E N A B A ST POLÍTICA DE SEGURIDAD DE — REVISIÓN: A  
  
Fedl  
  
ADQUISICIÓN, DESARROLLO Y RE  
MANTENIMIENTO DE LOS SISTEMAS DE A  
  
INFORMACIÓN —OOPÁGINAS | - 4delo  
  
Jefatura Departamento Asesoría Jurídica  
  
e En conjunto con el Encargado de Seguridad de la Información y la Jefatura de  
la Unidad Tecnologías de la Información, el Departamento de asesoría jurídica  
incorporará aspectos relacionados con el licenciamiento, la calidad del software  
y la seguridad de la información en los contratos con terceros para el desarrollo  
de software.  
  
4. Política  
  
4.1 Requisitos de seguridad de los sistemas de información  
  
Los sistemas de información de CENABAST, que incluyen la infraestructura,  
aplicaciones de negocio y aplicaciones desarrolladas por los usuarios deben tener  
incorporados los controles de seguridad correspondientes.  
  
Se deben identificar y acordar los requerimientos de seguridad que deben contener  
los sistemas de información de la organización antes de su desarrollo e  
implementación.  
  
Los requerimientos de seguridad para el desarrollo de los sistemas de información  
deben quedar documentados como parte del proceso de negocio del proyecto de  
implementación de sistemas de información.  
  
4.1.1 Análisis y especificación de los requisitos de seguridad  
  
e Los responsables por la provisión de soluciones deben crear y mantener una  
metodología que controle el ciclo completo de adquisición, desarrollo,  
mantenimiento y disposición seguro de soluciones de información e  
infraestructura.  
  
e Los requerimientos y los controles de seguridad deben ser proporcionales en  
costo y esfuerzo al valor de los activos de información involucrados y el daño  
potencial que podría resultar de una falla o ausencia de seguridad.  
  
e Los requerimientos de seguridad para la seguridad de la información y los  
procesos para implementar la seguridad deben ser integrados en las primeras  
etapas de los proyectos de sistemas de información (análisis y desarrollo),  
incorporando una etapa de evaluación de riesgos previa al diseño.  
  
\* Los controles introducidos en la etapa de diseño deben ser significativamente  
más baratos de implementar y mantener que aquellos incluidos durante o  
después de la implementación.  
  
e Si los productos son comprados, se debe realizar un proceso de prueba y  
adquisición formal, e incluir una evaluación de riesgos previo a su adquisición.

- POLÍTICA DE SEGURÍDAD DE  
C E N A B A S T ADQUISICIÓN, DESARROLLO Y  
  
POLÍTICA —  
  
40  
  
PO-Ss1-014  
  
MANTENIMIENTO DE LOS SISTEMAS DE  
  
— Fecha: 29 de julio de 2019 -  
  
INFORMACIÓN — PÁGINAS | 5deto  
  
Los contratos con el proveedor deben tratar los requerimientos de seguridad  
identificados.  
  
Cuando la funcionalidad de seguridad de un producto propuesto no satisface el  
requerimiento especificado, entonces se debe reconsiderar el riesgo introducido  
y los controles asociados antes de comprar el producto.  
  
Donde se suministra funcionalidad adicional y causa un riesgo de seguridad,  
éste debe ser desactivado o se debe revisar la estructura de control propuesta  
para determinar si se puede obtener alguna ventaja de la funcionalidad  
mejorada disponible.  
  
4.1.2 Protección de servicios de aplicación en redes públicas  
  
La información involucrada en los servicios de aplicación que pasan a través de redes  
públicas se debe proteger contra la actividad fraudulenta, la disputa de contratos y  
la información y modificación no autorizada, considerando lo siguiente:  
  
El nivel de confianza que requiere cada parte sobre la identidad manifestada de  
la otra, es decir, a través de la autenticación.  
  
Los procesos de autorización asociados a las personas que pudieran aprobar los  
contenidos de, emitir o firmar documentos de transacciones clave.  
  
Definir y cumplir con los requisitos de confidencialidad, integridad, prueba de  
despacho y recepción de documentos clave y el no repudio de contratos, es  
decir, asociados con los procesos de licitación y contratos.  
  
Los requisitos de protección de cualquier tipo de información confidencial.  
  
4.2 Seguridad en los procesos de desarrollo y soporte  
  
El desarrollo seguro de software debe considerar los siguientes aspectos:  
  
Seguridad del entorno de desarrollo  
  
Orientación sobre la seguridad del ciclo de vida del desarrollo de software  
Requisitos de seguridad en la fase de diseño  
  
Puntos de verificación de seguridad dentro de los hitos del proyecto  
Repositorios seguros  
  
Seguridad en el control de la versión  
  
Conocimiento de seguridad de aplicación necesario  
  
Capacidad de los desarrolladores de evitar, encontrar y solucionar la  
vulnerabilidad.

POLÍTICA — — | —cóme -| ross.o4  
C E N A B A S T POLÍTICA DE SEGURIDAD DE R£V¡$1€m 4\_\_gf ;  
  
ADQUISICIÓN, DESARROLLO Y AR ZE  
MANTENIMIENTO DE LOS SISTEMAS DE — 29 de julio de 2019  
  
INFORMACIÓN PÁGINAS. “| — 6de10  
  
4.2.1 Política de desarrollo seguro de software  
  
e Los procedimientos formales de control de cambios se deben documentar y  
hacer cumplir para minimizar la corrupción de los sistemas de información.  
  
e La introducción de sistemas nuevos y de cambios importantes en los  
sistemas existentes deben seguir un proceso formal de documentación,  
especificación, prueba, control de calidad e implementación con gestión.  
  
e — Este proceso debe incluir una evaluación de riesgos, análisis de los impactos  
de los cambios y especificación de los controles de seguridad necesarios.  
  
e Este proceso también debe garantizar que la seguridad y los procesos de  
control existentes no se exponen a riesgos o peligros, cuando se da acceso  
a los programadores de soporte sólo a aquellas partes del sistema necesarias  
para su trabajo y que existe acuerdo y aprobación formal para cualquier  
cambio.  
  
4.2.2 Revisión técnica de las aplicaciones tras efectuar cambios en el  
sistema operativo  
  
e Cuando se hacen cambios a las plataformas operacionales, las aplicaciones  
críticas de la organización deben ser revisadas y probadas para asegurar que  
no hay impacto adverso en la seguridad u operaciones.  
  
e Las plataformas de operación incluyen sistemas operativos, bases de datos  
y plataformas middleware. El control también debe ser aplicado a los  
cambios de las aplicaciones.  
  
4.2.3 Restricciones a los cambios en los paquetes de software  
  
e Solo se deben realizar cambios a los paquetes de software si es  
estrictamente necesario y estos deben ser controlados de manera rigurosa.  
  
\* En caso de considerarlo necesario, la modificación de paquetes de software  
suministrados por proveedores o de propiedad de la institución se deben  
previa autorización de la Jefatura de la Unidad de Tecnologías de la  
Información.  
  
+ Si los cambios son necesarios, el software original debe conservarse y los  
cambios aplicados a una copia designada.  
  
e Se debe implementar un proceso de gestión de actualizaciones de software,  
para garantizar que los parches aprobados y las actualizaciones de aplicación  
más recientes son instaladas para todo el software autorizado,

- POLÍTICA — PO-551-014  
CENABAST POLÍTICA DE SEGURIDAD DE 40  
ADQUISICIÓN, DESARROLLO Y TT  
MANTENIMIENTO DE LOS SISTEMAS DE — \* "2 29 <e duio de 2019  
INFORMACIÓN PÁGINAS —| -7de10  
  
Todos los cambios deben ser totalmente probados y documentados, para  
que se puedan volver a aplicar, si es necesario, para futuras actualizaciones  
del software.  
  
4.2.4 Uso de principios de ingeniería en protección de sistemas  
  
Se deben establecer, documentar y aplicar los procedimientos de ingeniería  
de sistemas de información segura en base a los principios de ingeniería de  
seguridad a las actividades de ingeniería del sistema de información interno.  
La seguridad se debe diseñar en todos los niveles de la arquitectura  
(negocios, datos, aplicaciones y tecnología) equilibrando la necesidad de la  
seguridad de la información con la necesidad de accesibilidad.  
  
Se debe analizar la tecnología nueva para conocer sus riesgos de seguridad  
y el diseño se deber revisar contra los patrones de ataque conocidos.  
  
Estos principios y los procedimientos de ingeniería establecidos se deben  
revisar de manera regular para asegurarse de que contribuyen de manera  
eficaz a las normas de seguridad mejoradas dentro del proceso de ingeniería.  
  
4.2.5 Seguridad de entornos de desarrolio  
  
La institución debe estabiecer y proteger los entornos de desarrollo seguro,  
de manera apropiada, para el desarrollo del sistema y los esfuerzos de  
integración que cubren todo el ciclo de desarrollo de sistemas.  
  
Un entorno de desarrollo seguro incluye a las personas, procesos y  
tecnologías asociadas con el desarrollo e integración de sistemas.  
  
La Unidad de Tecnologías de la Información en conjunto con el Encargado de  
Seguridad de la Información deben evaluar los riesgos asociados con las  
labores de desarrollo de sistemas individuales y establecer entornos de  
desarrollo seguro, para ello se debe considerar los siguientes elementos:  
  
o La sensibilidad de los datos que el sistema procesará, almacenará y  
transmitirá.  
  
o Los requisitos externos e internos correspondientes, es decir, de las  
normativas o políticas.  
  
o Controles de seguridad que ya ha implementado la institución y que  
soportan el desarrollo del sistema.  
  
o Confiabilidad del personal que trabaja en el entorno.  
o El grado de externalización asociado al desarrollo del sistema  
  
o La necesidad de contar con segregación entre distintos entornos de  
desarrollo

[ , .pO — PO-SsI-014  
CENABAST POLÍTICA DE SEGURIDAD DE m  
ADQUISICIÓN, DESARROLLO Y FU  
MANTENIMIENTO DE LOS SISTEMAS DE s i  
INFORMACIÓN 8 de 10  
  
o Control del acceso al entorno de desarroilo  
  
o Monitoreo del cambio al entorno y al código que ahí se almacena  
o Que los respaldos se almacenen en ubicaciones fuera del sitio  
  
o Control sobre el movimiento de datos desde y hacia el entorno.  
  
o La documentación requerida en las diferentes etapas de ciclo de vida de  
los sistemas.  
  
4.2.6 Externalización del desarrollo de software  
  
Para el caso que se considere la externalización del desarrollo de software, se  
debe supervisar y monitorear el desarrollo de éste, para lo cual se establecerá  
la documentación que contemplen los siguientes puntos:  
  
o Acuerdos de licencias, propiedad de código y derechos conferidos  
(Derechos de Propiedad Intelectual)  
  
o Requerimientos contractuales con respecto a la calidad del código y la  
existencia de garantías.  
  
o Documentos de certificación de la calidad y precisión del trabajo llevado  
a cabo por el proveedor, que incluyan auditorías, revisión de código para  
detectar códigos maliciosos, verificación del cumplimiento de los  
requerimientos de seguridad del software establecidos, etc.  
  
o Acuerdos de custodia de las fuentes de software (y cualquier otra  
información requerida) en caso de quiebre de la tercera parte.  
  
4.2.7 Pruebas de funcionalidad durante el desarrollo de los sistemas  
  
Los sistemas nuevos y actualizados se deben someter a pruebas y verificaciones  
exhaustivas durante los procesos de desarrollo, incluida la preparación de un  
programa de actividades detallado y entradas de pruebas y los resultados  
esperados bajo una variedad de condiciones.  
  
Las pruebas de aceptación independientes se deben realizar (tanto para los  
desarrollos internos y externalizados) para garantizar que el sistema funciona  
según se espera y sólo como se espera.  
  
El alcance de las pruebas debe ser en proporción a la importancia y naturaleza del  
sistema.

aa A A re  
CENABAST POLÍTICA DE SEGURIDAD DE — REVISIÓN —| '  
ADQUISICIÓN, DESARROLLO Y TT  
MANTENIMIENTO DE LOS SISTEMAS DE — \*":22 e  
INFORMACIÓN PÁGINAS  
  
4.2.8 Pruebas de aceptación  
  
\* LaJefatura de la Unidad de Tecnologías de la Información y el Encargado de  
Seguridad de la Información sugerirán criterios de aprobación para nuevos  
sistemas de información, actualizaciones y nuevas versiones, solicitando la  
realización de las pruebas necesarias antes de su aprobación definitiva.  
  
e Las pruebas de aceptación del sistema deben incluir las pruebas de los  
requisitos de seguridad de la información y la adherencia a las prácticas de  
desarrollo del sistema seguro.  
  
\* Las pruebas también se deben realizar en los componentes y sistemas  
integrados recibidos.  
  
\* Las pruebas se deben realizar en un entorno de pruebas realistas para  
garantizar que el sistema no introducirá vulnerabilidades al entorno de la  
organización y que las pruebas sean confiables.  
  
5. Difusión de la Política  
  
Se debe informar por medio de correo electrónico la revisión y/o actualización de la  
presente política, la que debe encontrarse publicada en la Intranet institucional de  
CENABAST, para su difusión interna.  
  
6. Revisión de la Política  
  
Las directrices y alcances contenidos en esta política son susceptibles de mejorar  
continuamente, por lo tanto, son factibles de someter a modificaciones,  
actualizaciones y cambios periódicos tendientes a mantener vigente y aplicable de  
acuerdo con las condiciones en que CENABAST se encuentre. Sin perjuicio de lo  
anterior, se establece que cada 2 años, al menos, esta política debe ser sometida a  
revisión y actualización.  
  
7. Glosario de términos  
  
N/A

CENABAST  
  
- POLÍTICA —  
  
| PO-SSI-014  
  
POLÍTICA DE SEGURIDAD DE  
ADQUISICIÓN, DESARROLLO Y  
MANTENIMIENTO DE LOS SISTEMAS DE  
  
INFORMACIÓN  
  
40  
  
10 de 10  
  
8. Control de Cambios.  
  
; Creación del documento “Políticas Específicas de  
10 14.12.2012 (E:Eíg:: Oa;t¿záxgdsreem:i$r;% Seguridad de la Información” que contiene todas las  
- . de la ?nformacióng políticas que abarcan los distintos dominios de la norma  
chilena 1ISO27001:2013.  
Pablo Fabres Fabres ifirarió -  
E Modificación a la estructura y contenido total del  
2.0 09.12.2017 Encargado de Seguridad PA r  
de la Información documento de políticas específicas.  
Pablo Fabres Fabres Se incluye política de protección de vida privada y datos  
3.0 27.11.2018 Encargado de Seguridad | sensibles, y política de prohibición de uso de software no  
de la Información autorizado.  
Se extrae la política del documento original “Políticas  
Pablo Fabres Fabres “ D aP .  
4.0 29.07.2019 Encargado de Seguridad Espe<á¡f¡cas de Seg'l:rld?cá de .|34 In;orn:jac¡g&ry I,(de1ando C  
de la Información este documento sól o el dominio de Adquisición,  
Desarrollo y Mantenimiento de Sistemas.  
  
10