POLÍTICA DE SEGURIDAD DE DESARROLLO

Junta Nacional de Jardines Infantiles
2021

TABLA DE CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. ROLES Y RESPONSABILIDADES 3
3.1. Unidad de TI 3
3.2. Encargado de seguridad de la Información 4
4. DEFINICIONES DE LA POLITICA 4
4.1. Requisitos de seguridad de los sistemas de información 4
4.2. Seguridad en los procesos de desarrollo y soporte 4
4.3. Control de cambios 5
4.4. Seguridad de entornos de desarrollo 5
4.5. Pruebas de funcionalidad durante el desarrollo de los sistemas 6
4.6. Pruebas de aceptación 6
4.7. Requerimientos de seguridad relacionados con redes públicas 7
4.8. Documentación anexa sobre ambientes e infraestructura de desarrollo. 7
5. PERIODICIDAD DE EVALUACIÓN Y REVISION 7
6. DIFUSIÓN 7
7. CONTROL DEL DOCUMENTO 8

1. OBJETIVO

Garantizar que la seguridad y el desarrollo de sistemas de información se diseñe e implemente dentro del ciclo de vida de desarrollo y seguridad de la información adecuados para asegurar la confidencialidad, integridad y disponibilidad de información de la institución y que asegure cumplir integralmente los requisitos para el desarrollo de los sistemas.

2. ALCANCE

El sistema de gestión de la información abarca a todos los sistemas y desarrollos informáticos que dan soporte a los productos estratégicos institucionales, 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.

La presente política es aplicable a la gestión de funcionarios de planta, contrata y el personal que se desempeñe en la calidad de honorarios y que formen parte de la JUNJI, y en general a cualquier otra persona o empresa que preste servicios y que se encuentre contratado por la institución.

Los controles de la normativa NCh-ISO 27001:2013 que aborda esta política de seguridad son:

- A.14.01.02: Aseguramiento de servicios de aplicación en redes públicas
- A.14.02.01: Política de desarrollo seguro
- A.14.02.06: Entorno de desarrollo seguro
- A.14.02.08: Prueba de seguridad del sistema
- A.14.02.09: Prueba de aprobación del sistema

3. ROLES Y RESPONSABILIDADES

3.1. Unidad de TI

- ✓ Aplicar las indicaciones que la presente normativa señala en relación con el desarrollo seguro de software y sistemas al interior de la Institución.
- ✓ Incorporar a las pruebas funcionales de los sistemas pruebas de seguridad.
- ✓ Velar que los distintos desarrollos de software o sistemas realizados cumplan con las definiciones técnicas y de arquitecturas con el fin de evitar encontrar vulnerabilidades técnicas.
- ✓ Identificar los requisitos de seguridad al inicio de cualquier proyecto de desarrollo.

- ✓ Dar cumplimiento a lo establecido en el "Procedimiento de Control de Cambios" (control 12.5.1) ante la implementación de nuevos sistemas o al cambio en sistemas en producción.
- ✓ Definir protocolos o controles (arquitectura, diseños, configuraciones, etc.) a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

3.2. Encargado de seguridad de la Información

- ✓ Definir en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos.

3.3. Comité de Seguridad de la Información:

- ✓ Asegurar que las materias abordadas en esta política se ejecutan y cumplan, promoviendo la difusión y sensibilización de las materias abordadas en esta política y promoviendo mejoras en el tiempo.

4. DEFINICIONES DE LA POLITICA

4.1. Requisitos de seguridad de los sistemas de información

Los sistemas de información de la institución, que incluyen la infraestructura, aplicaciones de negocio y aplicaciones desarrolladas por los usuarios o por terceros 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.

4.2. 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 vulnerabilidades.

4.3. Control de cambios

- Los procedimientos formales de control de cambios se deben documentar y hacer cumplir para minimizar la corrupción de los sistemas de información.
- 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.
- Este proceso debe incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios.
- 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.

4.4. Seguridad de entornos de desarrollo

- Se debe establecer 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 TI en conjunto con el Encargado de Seguridad de la Información deberán 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:
  - ✓ La sensibilidad de los datos que el sistema procesará almacenará y transmitirá.
  - ✓ Los requisitos externos e internos correspondientes, es decir, de las normativas o políticas.
  - ✓ Controles de seguridad que ya ha implementado la organización y que soportan el desarrollo del sistema.
  - ✓ Confiabilidad del personal que trabaja en el entorno.

- ✓ El grado de externalización asociado al desarrollo del sistema.
- ✓ Contar con segregación entre distintos entornos de desarrollo.
- ✓ Control del acceso al entorno de desarrollo.
- ✓ Monitoreo del cambio al entorno y al código que ahí se almacena.
- ✓ Control sobre el movimiento de datos desde y hacia el entorno.
- ✓ La documentación requerida en las diferentes etapas de ciclo de vida de los sistemas.

4.5. Pruebas de funcionalidad durante el desarrollo de los sistemas

- Los sistemas nuevos y actualizados se deberían 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 deberían 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 debería ser en proporción a la importancia y naturaleza del sistema.

4.6. Pruebas de aceptación

- La Jefatura de la Sección TI 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.
- Las pruebas de aceptación del sistema deberán 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 deberían realizar en los componentes y sistemas integrados recibidos.
- Las pruebas se deberán 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.

4.7. Requerimientos de seguridad relacionados con redes públicas

- Las transacciones de servicios deberán ser protegidas para evitar la transmisión incompleta de información, el enrutamiento incorrecto, la alteración, divulgación y duplicación no autorizada de mensajes.
- Los servicios de aplicación que pasan a través de redes públicas deben ser adecuadamente protegidos de actividades fraudulentas, protegiendo la confidencialidad, integridad y disponibilidad de la información que se transfiere a través de estos.

4.8. Documentación anexa sobre ambientes e infraestructura de desarrollo.

Como el desarrollo de aplicaciones y/o infraestructura es dinámico, es necesario contar con documentación que describa y entregue los lineamientos tanto a los equipos de desarrollo interno como proveedores externos para los requerimientos solicitados. En este contexto la Unidad de TI es la responsable de generar y actualizar la documentación respectiva. Forman parte de estos documentos entre otros, los siguientes documentos:

- ✓ Análisis de Arquitectura JUNJI
- ✓ Instalación DockerSwarm
- ✓ Instalación servidor Jenkins
- ✓ Instalación SonarQube y Nexus
- ✓ Versionamiento
- ✓ Despliegue de aplicaciones Javascript

5. PERIODICIDAD DE EVALUACIÓN Y REVISION

El presente documento será revisado cada dos años, o cuando la institución lo requiera, de manera de asegurar la continuidad e idoneidad del control, considerando los cambios que puedan producirse, tales como: enfoques a la gestión de seguridad de la información, cambios legales, normativos o estatutarios, cambios tecnológicos, recomendaciones frente a amenazas y vulnerabilidades, instrucciones que emanen de autoridades pertinentes, circunstancias de la Institución, entre otras.

6. DIFUSIÓN

La presente política deberá difundirse a todas y todos los funcionarios del Servicio a través del Correo Electrónico Institucional y/o publicado en la Intranet Institucional.

7. CONTROL DEL DOCUMENTO

HISTORIA DEL DOCUMENTO	
Nombre del Documento:	Política de Seguridad de Desarrollo
Creado por:	Jefes de Departamento y/o Secciones
Responsable del Documento:	Encargada de Seguridad de la Información
Fecha de Creación:	18/06/2019

CONTROL DE VERSIONES			
Versión	Fecha de Modificación	Motivo	**Páginas / secciones modificadas**
1.0	18-06-2019	Creación del documento	Todas
1.1	09-07-2019	Aprobación	Todas
1.2	16-08-2021	Actualización	Punto 1;3; Firmas; anexos

FIRMAS

Victor
Víctor (Sep 16, 2021 15:36 ADT)
Victor Campos Marchant
Encargado de Unidad Desarrollo TI

Claudio Henriquez
Claudio Henriquez (Sep 20, 2021 08:27 ADT)
Claudio Henriquez Rebolledo
Encargado de Unidad Continuidad Operativa TI

Marco Ibacacho O.
Marco Ibacache O. (Sep 20, 2021 08:30 ADT)
Marco Ibacache Olguín
Encargado de Sección de Tecnologías de Información
Encargado de Seguridad de la Información

Comité de Seguridad de la Información		
Nombre del Profesional	Departamento o Unidad	Revisión y Aprobación
Cristian Cerda Pérez	Comunicaciones y Ciudadanía	Cristian Cerda (Sep 15, 2021 09:48 ADT)
Enzo Marzán Oyarzún	Recursos Financieros	Enzo Marzán Oyarzún Enzo Marzán Oyarzún (Sep 14, 2021 16:48 ADT)
Javiera Osorio Estrada	Gestión y Desarrollo de las Personas	Javiera Osorio Estrada Javiera Osorio Estrada (Sep 15, 2021 11:06 ADT)
Julio Saavedra Rojas	Fiscalía y Asesoría Jurídica	
Constanza Sabater Orellana	Calidad Educativa	
Patricio Reyes Martínez	Unidad de Tecnologías de la Información	Patricio Reyes Patricio Reyes (Sep 13, 2021 17:33 ADT)

JUNJI_A.14.1_Política de Seguridad de Desarrollo_V1.2

Final Audit Report 2021-09-20

Created:	2021-09-13
By:	Patricio Reyes (PREYES@JUNJI.CL)
Status:	Signed
Transaction ID:	CBJCHBCAABAA439jf4JwjXnRagr4qKI9uIJIvtEUNohe

"JUNJI_A.14.1_Política de Seguridad de Desarrollo_V1.2" History

Document created by Patricio Reyes (PREYES@JUNJI.CL)
2021-09-13 - 8:30:34 PM GMT- IP address: 190.22.12.38

Document e-signed by Patricio Reyes (PREYES@JUNJI.CL)
Signature Date: 2021-09-13 - 8:33:02 PM GMT - Time Source: server- IP address: 190.22.12.38

Document emailed to Julio Saavedra (jasaavedra@junji.cl) for signature
2021-09-13 - 8:33:05 PM GMT

Email viewed by Julio Saavedra (jasaavedra@junji.cl)
2021-09-14 - 1:32:56 PM GMT- IP address: 186.11.83.78

Document e-signed by Julio Saavedra (jasaavedra@junji.cl)
Signature Date: 2021-09-14 - 1:33:37 PM GMT - Time Source: server- IP address: 186.11.83.78

Document emailed to Constanza Sabater O. (csabater@junji.cl) for signature
2021-09-14 - 1:33:39 PM GMT

Email viewed by Constanza Sabater O. (csabater@junji.cl)
2021-09-14 - 2:26:11 PM GMT- IP address: 201.215.178.119

Document e-signed by Constanza Sabater O. (csabater@junji.cl)
Signature Date: 2021-09-14 - 2:26:38 PM GMT - Time Source: server- IP address: 201.215.178.119

Document emailed to Enzo Marzán Oyarzún (emarzan@junji.cl) for signature
2021-09-14 - 2:26:40 PM GMT

Email viewed by Enzo Marzán Oyarzún (emarzan@junji.cl)
2021-09-14 - 7:47:55 PM GMT- IP address: 201.239.120.72

Adobe Sign

Document e-signed by Enzo Marzán Oyarzún (emarzan@junji.cl)
Signature Date: 2021-09-14 - 7:48:34 PM GMT - Time Source: server- IP address: 201.239.120.72

Document emailed to Cristian Cerda (ccerda@junji.cl) for signature
2021-09-14 - 7:48:37 PM GMT

Email viewed by Cristian Cerda (ccerda@junji.cl)
2021-09-15 - 12:47:36 PM GMT- IP address: 200.111.176.225

Document e-signed by Cristian Cerda (ccerda@junji.cl)
Signature Date: 2021-09-15 - 12:48:15 PM GMT - Time Source: server- IP address: 200.111.176.225

Document emailed to Javiera Osorio Estrada (jfosorio@junji.cl) for signature
2021-09-15 - 12:48:17 PM GMT

Email viewed by Javiera Osorio Estrada (jfosorio@junji.cl)
2021-09-15 - 12:56:37 PM GMT- IP address: 181.42.27.29

Document e-signed by Javiera Osorio Estrada (jfosorio@junji.cl)
Signature Date: 2021-09-15 - 2:06:18 PM GMT - Time Source: server- IP address: 181.226.100.222

Document emailed to Víctor (vcampos@junji.cl) for signature
2021-09-15 - 2:06:20 PM GMT

Email viewed by Víctor (vcampos@junji.cl)
2021-09-16 - 6:35:58 PM GMT- IP address: 181.42.41.125

Document e-signed by Víctor (vcampos@junji.cl)
Signature Date: 2021-09-16 - 6:36:11 PM GMT - Time Source: server- IP address: 181.42.41.125

Document emailed to Claudio Henriquez (cahenriquez@junji.cl) for signature
2021-09-16 - 6:36:13 PM GMT

Email viewed by Claudio Henriquez (cahenriquez@junji.cl)
2021-09-20 - 11:27:08 AM GMT- IP address: 200.111.176.225

Document e-signed by Claudio Henriquez (cahenriquez@junji.cl)
Signature Date: 2021-09-20 - 11:27:31 AM GMT - Time Source: server- IP address: 200.111.176.225

Document emailed to Marco Ibacache O. (mibacache@junji.cl) for signature
2021-09-20 - 11:27:33 AM GMT

Email viewed by Marco Ibacache O. (mibacache@junji.cl)
2021-09-20 - 11:28:37 AM GMT- IP address: 200.111.176.225

Document e-signed by Marco Ibacache O. (mibacache@junji.cl)
Signature Date: 2021-09-20 - 11:30:00 AM GMT - Time Source: server- IP address: 200.111.176.225

Adobe Sign

Agreement completed.

2021-09-20 - 11:30:00 AM GMT

Adobe Sign