



POLÍTICA DE SEGURIDAD DE OPERACIONES

Junta Nacional de Jardines Infantiles
2021

TABLA DE CONTENIDO

1. OBJETIVO	3
2. ALCANCE	3
3. ROLES Y RESPONSABILIDADES	3
4. DEFINICIONES DE LA POLITICA	4
4.1. Separación de entornos de desarrollo, prueba y producción	4
4.2. Controles de código malicioso	5
4.3. Registro y gestión de eventos	5
4.4. Protección de los registros de información	5
4.5. Registros de actividad del administrador y operador del sistema	6
4.6. Sincronización de relojes	6
4.7. Gestión de vulnerabilidad técnica	6
4.8. Restricciones en la instalación de software	7
5. PERIODICIDAD DE EVALUACIÓN Y REVISION	7
6. DIFUSIÓN	7
7. CONTROL DEL DOCUMENTO	8



1. OBJETIVO

Garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

2. ALCANCE

Esta política aplica a las instalaciones de procesamiento de información existentes en la institución y que dan soporte a todos los procesos de provisión de bienes y servicios.

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

- A.12.01.04: Separación de los ambientes de desarrollo, prueba y operacionales
- A.12.02.01: Controles contra código malicioso
- A.12.04.01: Registro de Evento
- A.12.04.03: Registro del administrador y del operador
- A.12.04.04: Sincronización de Relojes
- A.12.06.01: Gestión de las vulnerabilidades técnicas
- A.12.06.02: Restricciones sobre la instalación de software

3. ROLES Y RESPONSABILIDADES

• Jefatura de la Sección de Tecnologías de Información

- ✓ Definir controles de prevención y recuperación para protegerse contra códigos maliciosos.
- ✓ Desarrollar planes adecuados de concientización de usuarios en materia de seguridad, amenazas de códigos maliciosos, controles de acceso al sistema y administración de cambios.
- ✓ Deben definir y elaborar los controles para la protección de los sistemas de monitoreo y los registros producidos y almacenados.

Establecer una gestión de vulnerabilidades técnicas de los activos de información junto con Encargado de Seguridad de la Información.

• Encargado de la Oficina de Operaciones

- ✓ Definir controles de prevención y recuperación para protegerse contra códigos maliciosos.
- ✓ Desarrollar planes adecuados de concientización de usuarios en materia de seguridad, amenazas de códigos maliciosos, controles de acceso al sistema y administración de cambios.



- ✓ Deben definir y elaborar los controles para la protección de los sistemas de monitoreo y los registros producidos y almacenados.
- ✓ Sincronizar los relojes de todos los elementos relevantes de redes y sistemas de procesamiento de la información. Realizar controles que permitan la validación del código.
- **Encargado de Seguridad de la Información**
 - ✓ Debe tener acceso a los sistemas y a los registros de actividad, con el objetivo de colaborar en el control y efectuar recomendaciones de mejora.
 - ✓ Establecer una gestión de vulnerabilidades técnicas de los activos de información junto con la Sección TI.

4. DEFINICIONES DE LA POLITICA

4.1. Separación de entornos de desarrollo, prueba y producción

- Los ambientes para desarrollo, prueba y producción se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.
- Los ambientes de desarrollo, prueba y producción, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo.
- Se deben desalentar las modificaciones a los paquetes de software, limitándose a los cambios necesarios, los que deben ser controlados de manera estricta.
- El acceso a los ambientes de desarrollo, prueba y producción debe seguir una adecuada segregación, evitando que usuarios con perfil de desarrollo tengan acceso a los ambientes de producción.



4.2. Controles de código malicioso

- El **Encargado de la Oficina de Operaciones** en conjunto a la **Jefatura de la Sección de TI**, definirán controles de prevención y recuperación para protegerse contra códigos maliciosos.
- La **Sección de TI** será responsable de implementar y administrar dichos controles.
- El **Encargado de la Oficina de Operaciones** será el responsable de desarrollar planes adecuados de concientización de usuarios en materia de seguridad, amenazas de códigos maliciosos, controles de acceso al sistema y administración de cambios.

4.3. Registro y gestión de eventos

- Debe monitorearse el uso de las instalaciones de procesamiento de la información, debiendo generar, mantener y revisar registros de las actividades de los usuarios; excepciones, faltas y eventos de seguridad de la información de manera regular.
- La **Oficina de Operaciones** debe implementar una gestión de eventos que contemple las siguientes actividades cuando corresponda:
 - ✓ Elaboración del registro de fallas reportadas por usuarios, programas y sistemas, con el objetivo de prevenir su repetición o facilitar su resolución en caso de reincidencia.
 - ✓ Registro y revisión de las medidas correctivas tomadas.
 - ✓ Revisión de registros de fallas para asegurar que los problemas han sido satisfactoriamente resueltos.
 - ✓ Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.
 - ✓ Ejecución de operaciones críticas.
 - ✓ Cambios a información crítica.
- El **Encargado de Seguridad de la Información** debe tener acceso a los sistemas y a los registros de actividad, con el objetivo de colaborar en el control y efectuar recomendaciones de mejora.

4.4. Protección de los registros de información

- Tanto los sistemas de monitoreo, como la información registrada durante las actividades de monitoreo deben ser protegidos contra la alteración indebida y el acceso no autorizado.
- El **Encargado de la Oficina de Operaciones** en conjunto con la **Jefatura de la Sección de TI**, deben definir y elaborar los controles para la protección de los sistemas de monitoreo y los registros producidos y almacenados.
- Es responsabilidad de la **Sección de TI** implementar los controles definidos.



- Se producirán revisiones regulares a los registros de eventos que generan las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

4.5. Registros de actividad del administrador y operador del sistema

- Se deben registrar, respaldar, proteger y revisar regularmente, las actividades del administrador y operadores de las distintas plataformas tecnológicas. El Log de actividades debe incluir al menos:
 - ✓ Identificación del equipo.
 - ✓ Horario de arranque y finalización de los procesos del sistema.
 - ✓ Errores del sistema y acciones críticas realizadas.
 - ✓ Cuenta del operador que realizó la actividad.
 - ✓ Sistemas y procesos involucrados.
- Los registros o logs de sistemas podrán ser revisados por entidades externas para validarlos contra los procedimientos operativos.

4.6. Sincronización de relojes

- Los relojes de todos los elementos relevantes de redes y sistemas de procesamiento de la información deben estar configurados apropiadamente y sincronizados respecto de una fuente de tiempo precisa.
- **La Oficina de Operaciones** se encargará de implementar este control.

4.7. Gestión de vulnerabilidad técnica

- Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información críticos que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.
- Debe obtenerse información oportuna relacionada con las vulnerabilidades técnicas de los sistemas de información y equipos de red utilizados por la institución, evaluar la exposición a dichas vulnerabilidades y adoptar los controles adecuados para manejar los riesgos.
- **El Encargado de Seguridad de la Información**, junto a **la Jefatura de la Sección de TI**, deben establecer una gestión de vulnerabilidades técnicas de los activos críticos de información.



4.8. Restricciones en la instalación de software

- Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
- Las normas que regirán la instalación de software por los usuarios serán establecidas e implementadas. Los funcionarios(as) no estarán facultados para realizar la instalación y utilización de software no autorizado en sus estaciones de trabajo ni en las plataformas tecnológicas que soportan los sistemas de información de la Institución.

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 Operaciones.
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
1.3	10-08-2021	Actualización	Firmas

FIRMAS	
 <small>Claudio Henriquez (Sep 15, 2021 11:06 ADT)</small> Claudio Henriquez Rebolledo Encargado de Unidad Continuidad Operativa TI	 <small>Marco Ibacache (Sep 15, 2021 11:40 ADT)</small> Marco Ibacache Olguín Encargado de Sección de Tecnologías de Información Encargado de Seguridad de la Información

POLÍTICA DE SEGURIDAD DE OPERACIONES
JUNTA NACIONAL DE JARDINES INFANTILES

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 09:46 ADT)
Enzo Marzán Oyarzún	Recursos Financieros	 Enzo Marzán Oyarzún (Sep 14, 2021 16:46 ADT)
Javiera Osorio Estrada	Gestión y Desarrollo de las Personas	 Javiera Osorio Estrada (Sep 15, 2021 11:05 ADT)
Julio Saavedra Rojas	Fiscalía y Asesoría Jurídica	
Constanza Sabater Orellana	Calidad Educativa	
Patricio Reyes Martínez	Unidad de Tecnologías de la Información	 Patricio Reyes (Sep 13, 2021 15:40 ADT)



JUNJI_A.12_Política de Seguridad de Operaciones_V1.2

Final Audit Report

2021-09-15

Created:	2021-09-13
By:	Patricio Reyes (PREYES@JUNJI.CL)
Status:	Signed
Transaction ID:	CBJCHBCAABAAPRfWPjDDdkBgRmLKfD6sNstn_DJLoLn

History

-  Document created by Patricio Reyes (PREYES@JUNJI.CL)
2021-09-13 - 6:37:15 PM GMT- IP address: 190.22.12.38
-  Document e-signed by Patricio Reyes (PREYES@JUNJI.CL)
Signature Date: 2021-09-13 - 6:40:27 PM GMT - Time Source: server- IP address: 190.22.12.38
-  Document emailed to Julio Saavedra (jasaavedra@junji.cl) for signature
2021-09-13 - 6:40:31 PM GMT
-  Email viewed by Julio Saavedra (jasaavedra@junji.cl)
2021-09-14 - 1:30:29 PM GMT- IP address: 186.11.83.78
-  Document e-signed by Julio Saavedra (jasaavedra@junji.cl)
Signature Date: 2021-09-14 - 1:31:35 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 - 1:31:37 PM GMT
-  Email viewed by Constanza Sabater O. (csabater@junji.cl)
2021-09-14 - 2:24:47 PM GMT- IP address: 201.215.178.119
-  Document e-signed by Constanza Sabater O. (csabater@junji.cl)
Signature Date: 2021-09-14 - 2:25:20 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 - 2:25:22 PM GMT
-  Email viewed by Enzo Marzán Oyarzún (emarzan@junji.cl)
2021-09-14 - 7:45:41 PM GMT- IP address: 201.239.120.72



Document e-signed by Enzo Marzán Oyarzún (emarzan@junji.cl)

Signature Date: 2021-09-14 - 7:46:29 PM GMT - Time Source: server- IP address: 201.239.120.72



Document emailed to Cristian Cerda (ccerda@junji.cl) for signature

2021-09-14 - 7:46:32 PM GMT



Email viewed by Cristian Cerda (ccerda@junji.cl)

2021-09-15 - 12:45:56 PM GMT- IP address: 200.111.176.225



Document e-signed by Cristian Cerda (ccerda@junji.cl)

Signature Date: 2021-09-15 - 12:46:45 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 - 12:46:47 PM GMT



Email viewed by Javiera Osorio Estrada (jfosorio@junji.cl)

2021-09-15 - 2:03:58 PM GMT- IP address: 181.226.100.222



Document e-signed by Javiera Osorio Estrada (jfosorio@junji.cl)

Signature Date: 2021-09-15 - 2:05:30 PM GMT - Time Source: server- IP address: 181.226.100.222



Document emailed to Claudio Henriquez (cahenriquez@junji.cl) for signature

2021-09-15 - 2:05:33 PM GMT



Email viewed by Claudio Henriquez (cahenriquez@junji.cl)

2021-09-15 - 2:06:01 PM GMT- IP address: 200.111.176.225



Document e-signed by Claudio Henriquez (cahenriquez@junji.cl)

Signature Date: 2021-09-15 - 2:06:29 PM GMT - Time Source: server- IP address: 200.111.176.225



Document emailed to Marco Ibacache (mibacache@junji.cl) for signature

2021-09-15 - 2:06:31 PM GMT



Email viewed by Marco Ibacache (mibacache@junji.cl)

2021-09-15 - 2:39:59 PM GMT- IP address: 186.11.24.210



Document e-signed by Marco Ibacache (mibacache@junji.cl)

Signature Date: 2021-09-15 - 2:40:52 PM GMT - Time Source: server- IP address: 186.11.24.210



Agreement completed.

2021-09-15 - 2:40:52 PM GMT



Adobe Sign