



POLÍTICA DE SEGURIDAD DE REDES

Junta Nacional de Jardines Infantiles
2021

TABLA DE CONTENIDO

1. OBJETIVO	3
2. ALCANCE	3
3. ROLES Y RESPONSABILIDADES	3
3.1. Jefe de Sección TI	3
3.2. Sección TI	3
3.3. Encargado de Seguridad de la Información	4
4. DEFINICIONES DE LA POLITICA	4
4.1. Controles de red	4
4.2. Mecanismos de seguridad asociados a servicios en red	4
4.3. Segregación de redes	4
5. PERIODICIDAD DE EVALUACIÓN Y REVISION	5
6. DIFUSIÓN	5
7. CONTROL DEL DOCUMENTO	6



1. OBJETIVO

Garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.

2. ALCANCE

El sistema de gestión de la información abarca las instalaciones de red y comunicaciones existentes en la institución y que dan soporte a todos los procesos de provisión de bienes y servicios de la institución.

La presente política es aplicable a la gestión de funcionarios de planta, contrata y el personal que se desempeña 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.13.01.01: Controles de red
- A.13.01.02: Seguridad de los servicios de red
- A.13.01.03: Separación en las redes

3. ROLES Y RESPONSABILIDADES

3.1. Jefe de Sección TI

- ✓ Definir junto al Encargado de la Seguridad de la Información los procedimientos y controles que garanticen la integridad, confidencialidad y disponibilidad de las comunicaciones.
- ✓ Establecer el perímetro de seguridad necesario para proteger los distintos segmentos de red, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

3.2. Sección TI

- ✓ Establecer el perímetro de seguridad necesario para proteger los segmentos definidos para la Plataforma Tecnológica, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- ✓ Garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.



3.3. Encargado de Seguridad de la Información

- ✓ Definir junto a la Jefatura de la Unidad TIC los procedimientos y controles que garanticen la integridad, confidencialidad y disponibilidad de las comunicaciones.
- ✓ Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

4. DEFINICIONES DE LA POLITICA

4.1. Controles de red

El Encargado de Seguridad de la Información en conjunto con **la Jefatura de la Sección TI**, definirán los controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la institución contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas y para proteger los sistemas conectados, implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.
- La Jefatura de la Unidad TI deberá implementar dichos controles.

4.2. Mecanismos de seguridad asociados a servicios en red

El Encargado de Seguridad de la Información en conjunto a **la Jefatura de la Sección de TI** definirán el proceso y controles para identificar los dispositivos de seguridad, niveles de servicio y sus requerimientos operativos y de seguridad, e incluirlos en contratos de red, sean estos internos o externos.

4.3. Segregación de redes

- Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.
- Se definirán y documentarán los perímetros de seguridad que sean convenientes.
- La plataforma tecnológica de la institución que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. **La Sección TI** es el área encargada



POLÍTICA DE SEGURIDAD DE REDES JUNTA NACIONAL DE JARDINES INFANTILES

de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

- Los perímetros se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios.
- Se deben implementar y establecer mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la institución.
- Es responsabilidad de **la Sección TI** garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

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.



POLÍTICA DE SEGURIDAD DE REDES
JUNTA NACIONAL DE JARDINES INFANTILES

7. CONTROL DEL DOCUMENTO

HISTORIA DEL DOCUMENTO	
Nombre del Documento:	Política de Seguridad de Redes
Creado por:	Jefes de Departamento y/o Secciones
Responsable del Documento:	Encargada 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	10-08-2021	Actualización	Firmas

FIRMAS	
 <small>Claudio Henriquez (Sep 15, 2021 11:36 ADT)</small> Claudio Henriquez Rebolledo Encargado de Unidad Continuidad Operativa TI	 <small>Marco Ibacache (Sep 15, 2021 11:41 ADT)</small> Marco Ibacache Olguín Encargado de Sección de Tecnologías de Información Encargado de Seguridad de la Información



POLÍTICA DE SEGURIDAD DE REDES
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 09:47 ADT)
Enzo Marzán Oyarzún	Recursos Financieros	 Enzo Marzán Oyarzún (Sep 14, 2021 16:47 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 15:57 ADT)



JUNJI_A.13.1_Política Seguridad de Redes_V1.2

Final Audit Report

2021-09-15

Created:	2021-09-13
By:	Patricio Reyes (PREYES@JUNJI.CL)
Status:	Signed
Transaction ID:	CBJCHBCAABAAygb3-PweO88OHRnOuqomQQIWcdIH61Ri

"JUNJI_A.13.1_Política Seguridad de Redes_V1.2" History

-  Document created by Patricio Reyes (PREYES@JUNJI.CL)
2021-09-13 - 6:53:27 PM GMT- IP address: 190.22.12.38
-  Document e-signed by Patricio Reyes (PREYES@JUNJI.CL)
Signature Date: 2021-09-13 - 6:57:51 PM GMT - Time Source: server- IP address: 190.22.12.38
-  Document emailed to Julio Saavedra (jasaavedra@junji.cl) for signature
2021-09-13 - 6:57:56 PM GMT
-  Email viewed by Julio Saavedra (jasaavedra@junji.cl)
2021-09-14 - 1:31:47 PM GMT- IP address: 186.11.83.78
-  Document e-signed by Julio Saavedra (jasaavedra@junji.cl)
Signature Date: 2021-09-14 - 1:32:45 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 - 1:32:47 PM GMT
-  Email viewed by Constanza Sabater O. (csabater@junji.cl)
2021-09-14 - 2:25:30 PM GMT- IP address: 201.215.178.119
-  Document e-signed by Constanza Sabater O. (csabater@junji.cl)
Signature Date: 2021-09-14 - 2:25:56 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 - 2:25:59 PM GMT
-  Email viewed by Enzo Marzán Oyarzún (emarzan@junji.cl)
2021-09-14 - 7:46:39 PM GMT- IP address: 201.239.120.72



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

Signature Date: 2021-09-14 - 7:47:44 PM GMT - Time Source: server- IP address: 201.239.120.72



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

2021-09-14 - 7:47:47 PM GMT



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

2021-09-15 - 12:46:57 PM GMT- IP address: 200.111.176.225



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

Signature Date: 2021-09-15 - 12:47:28 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 - 12:47:30 PM GMT



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

2021-09-15 - 12:56:35 PM GMT- IP address: 181.42.27.29



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

Signature Date: 2021-09-15 - 2:05:56 PM GMT - Time Source: server- IP address: 181.226.100.222



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

2021-09-15 - 2:05:58 PM GMT



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

2021-09-15 - 2:06:36 PM GMT- IP address: 200.111.176.225



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

Signature Date: 2021-09-15 - 2:06:53 PM GMT - Time Source: server- IP address: 200.111.176.225



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

2021-09-15 - 2:06:55 PM GMT



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

2021-09-15 - 2:41:08 PM GMT- IP address: 186.11.24.210



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

Signature Date: 2021-09-15 - 2:41:43 PM GMT - Time Source: server- IP address: 186.11.24.210



Agreement completed.

2021-09-15 - 2:41:43 PM GMT



Adobe Sign