POLÍTICA DE SEGURIDAD FÍSICA Y DEL AMBIENTE

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 5
4.1. PERÍMETRO DE SEGURIDAD FÍSICA 5
4.2. CONTROLES FÍSICOS DE ENTRADA A LAS ÁREAS SEGURAS 5
4.3. UBICACION Y PROTECCIÓN DE LOS EQUIPOS 6
4.4. MANTENIMIENTO DE LOS EQUIPOS 7
4.5. ELIMINACIÓN O REUTILIZACIÓN SEGURA DE EQUIPOS 7
4.6. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS 8
5. PERIODICIDAD DE EVALUACIÓN Y REVISION 9
6. DIFUSIÓN 9
7. GLOSARIO 10
8. CONTROL DEL DOCUMENTO 11

1. OBJETIVO

El presente documento establece las directrices para evitar el acceso físico no autorizado, daños e interferencias a los activos de información y a las instalaciones de procesamiento de la información de la Junta Nacional de Jardines Infantiles (JUNJI).

2. ALCANCE

El sistema de gestión de la información abarca a todas las oficinas / Instalaciones asociadas a la Dirección Nacional de JUNJI, referidos al procesamiento de información, ubicados en:

- Marchant Pereira 726
- Darío Urzua 1938
- Salvador Allende 105
- Morandé 226 (pisos 5, 6 y 7)

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.11.01.01 Perímetro de seguridad física
A.11.02.01 Ubicación y protección del equipamiento
A.11.02.04 Mantenimiento del Equipamiento
A.11.02.08 Equipo del usuario desatendido
A.11.02.09 Política de escritorio y pantalla limpios.

3. ROLES Y RESPONSABILIDADES

3.1. Jefatura Departamento Recursos Financieros

Definir perímetros de seguridad de acuerdo con los requisitos de seguridad de los activos dentro del perímetro y los resultados de la evaluación de riesgos. Implementar un área de recepción atendida por una persona u otros medios efectivos para controlar el acceso físico a las instalaciones. Proveer y gestionar los dispositivos y mecanismos de control de acceso físico a las dependencias e instalaciones de procesamiento de la información de la institución.

3.2. Las Jefaturas de Área

- ✓ Deberá proteger las áreas seguras con controles de entrada adecuados para garantizar que sólo se permita el acceso al personal autorizado.
- ✓ Revisar y actualizar de manera regular los derechos de acceso a las áreas seguras y revocarlos cuando sea necesario

3.3. Sección TI

- ✓ Emplazar y proteger los equipos para reducir los riesgos asociados a las amenazas ambientales y las oportunidades de acceso no autorizado.
- ✓ Mantener correctamente los equipos críticos para garantizar su disponibilidad e integridad continuas.
- ✓ Eliminar, destruir o sobrescribir todos los datos contenidos en los equipos antes de darlos de baja, para ello deberá utilizar técnicas que impidan la recuperación de la información, en lugar de recurrir al formateo tradicional.

3.4. Funcionarios JUNJI

- ✓ Asegurarse de que los equipos no supervisados cuentan con la protección adecuada de manera de poder evitar el acceso indebido a sistemas y/o a la información contenida en él.

4. DEFINICIONES DE LA POLITICA

4.1. PERÍMETRO DE SEGURIDAD FÍSICA

a) La **Jefatura del Departamento de Recursos Financieros** deberá definir perímetros de seguridad de acuerdo con los requisitos de seguridad de los activos dentro del perímetro y los resultados de la evaluación de riesgos y

b) Las Áreas Seguras deberán ser físicamente sólidas considerando: techo, paredes y piso; las puertas y ventanas se deben cerrar correctamente cuando se dejan sin vigilancia y se deberá considerar una protección externa para las ventanas, en particular si se ubican a nivel del suelo.

c) La **Jefatura del Departamento de Recursos Financieros** deberá implementar un área de recepción atendida por una persona u otros medios efectivos para controlar el acceso físico a las instalaciones; el acceso a los sitios y a las distintas dependencias se deberá restringir solo al personal autorizado y tomar las medidas correspondientes para el acceso de visitas o personal ajeno a la institución.

d) Se deben utilizar barreras físicas donde corresponda para evitar el acceso físico no autorizado.

e) Todas las puertas contra incendios existentes en el perímetro de seguridad deben ser monitoreadas y probadas en conjunto con las paredes para establecer el nivel de resistencia necesario de acuerdo con las normas correspondientes; deben operar de acuerdo con el código de incendios local y a prueba de fallos.

f) **La Jefatura de la sección de Tecnologías de la Información** deberá proveer y gestionar los dispositivos y mecanismos de control de acceso físico a las dependencias e instalaciones de procesamiento de la información de la institución.

4.2. CONTROLES FÍSICOS DE ENTRADA A LAS ÁREAS SEGURAS

a) **Las Jefaturas** que tengan dentro de sus responsabilidades el resguardado de áreas seguras deberán protegerlas con controles de entrada adecuados para garantizar que sólo se permita el acceso al personal autorizado.

b) Se deberá implementar y mantener un registro de entrada y salida de las visitas (detallando al menos nombre, fecha y la hora) y supervisar a todas las visitas a menos que su acceso haya sido aprobado anteriormente; sólo se les debe otorgar acceso para propósitos específicos y autorizados de acuerdo con las instrucciones de los requisitos de seguridad del área y a los procedimientos de emergencia. Se debe autenticar la identidad de las visitas con un medio adecuado.

c) Está prohibido el acceso a funcionarios no autorizados a aquellas áreas declaradas como seguras o restringidas.
d) El personal de aseo debe estar identificado con su uniforme de la empresa mientras desarrollen sus labores.
e) Se debe otorgar acceso restringido a los proveedores a las áreas seguras sólo cuando sea necesario. Este acceso se debe autorizar y monitorear.
f) **Las Jefaturas** que tengan dentro de sus responsabilidades el resguardado de las áreas seguras deberán revisar y actualizar de manera regular los derechos de acceso a las áreas seguras y revocarlos cuando sea necesario**.**
g) El acceso al Datacenter se debe restringir a las personas autorizadas mediante la implementación de controles de acceso adecuados.

4.3. UBICACION Y PROTECCIÓN DE LOS EQUIPOS

La Jefatura de la sección de Tecnologías de la Información deberá entregar los lineamientos para emplazar y proteger los equipos para reducir los riesgos asociados a las amenazas ambientales y las oportunidades de acceso no autorizado, considerando lo siguiente:

a) Los equipos se deben emplazar en un lugar determinado para minimizar el acceso innecesario a las áreas de trabajo.
b) Se deben adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales, es decir, robos, incendios, humo, agua, polvo, vibraciones, efectos químicos, interferencia del suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
c) Las instalaciones de procesamiento de información que manejan datos sensibles deben estar ubicados de manera estratégica para reducir el riesgo de acceso de personas no autorizadas.
d) Se deben monitorear las condiciones ambientales como la temperatura y la humedad de manera de evitar que éstas puedan afectar adversamente a la operación de las instalaciones de procesamiento de información y los activos de información almacenados en áreas seguras.
e) Está prohibido comer, beber y/o fumar en la proximidad o dentro de las instalaciones de procesamiento de información.
f) **Los funcionarios** deben asegurarse de que los equipos no supervisados cuentan con la protección adecuada de manera de poder evitar el acceso indebido a sistemas y/o a la información contenida en él.

4.4. MANTENIMIENTO DE LOS EQUIPOS

La Sección de Tecnologías de la Información deberá mantener correctamente los equipos críticos para garantizar su disponibilidad e integridad continuas. Para ello se deberán considerar las siguientes pautas para la mantención de los equipos críticos:

a) Las mantenciones de los equipos se deben realizar de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor.
b) Solo el personal autorizado debe realizar reparaciones y labores de mantenimiento y servicio a los equipos.
c) Se deben mantener registros de todas las fallas y mantenciones preventivas y correctivas.
d) Se deben implementar controles adecuados cuando se programa la mantención de equipos, considerando si ésta la realizará personal externo a la organización; donde sea necesario se debe eliminar la información confidencial del equipo, o bien la debería realizar funcionarios de soporte pertenecientes al área TI
e) Se debe cumplir con todos los requisitos de mantención impuestos por las políticas de seguros, según corresponda.
f) Una vez realizada la mantención de un equipo, luego de volver a funcionamiento, el equipo debe ser inspeccionado para garantizar que no ha sido adulterado y que funciona adecuadamente.

4.5. ELIMINACIÓN O REUTILIZACIÓN SEGURA DE EQUIPOS

a) **La Sección de Tecnologías de Información** deberá eliminar, destruir o sobrescribir todos los datos contenidos en los equipos antes de darlos de baja, para ello deberá utilizar técnicas que impidan la recuperación de la información, en lugar de recurrir al formateo tradicional.
b) En el caso de la reutilización de equipos, se debe verificar la eliminación de toda aquella información que no debería tener acceso el nuevo usuario.
c) Se debe considerar que además del borrado seguro del disco, el cifrado del disco completo reduce el riesgo de divulgar información confidencial cuando se elimina o vuelve a implementar el equipo, siempre que:
    i. El proceso de cifrado sea lo suficientemente fuerte y que cubra a todo el disco (incluido el espacio despejado, los archivos de intercambio, etc.)

ii. Las claves de cifrado sean lo suficientemente largas como para resistir los ataques de fuerza bruta.
iii. Las claves de cifrado en sí se mantengan de manera confidencial (es decir, que nunca se almacenen en el mismo disco).

4.6. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Ante la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información, **los funcionarios** deben adoptar buenas prácticas en el uso de documentos físicos y de medios de almacenamiento extraíbles, así como también mantener pantallas despejadas en las instalaciones de procesamiento de información, considerando que:

a) La información sensible o crítica para la institución que esté almacenada en medios electrónicos o papel, debe mantenerse guardada bajo llave cuando no se necesite, especialmente cuando la oficina esté desocupada.
b) Los computadores y terminales deben estar protegidos con un mecanismo de bloqueo de pantalla y teclado mediante una contraseña, token o mecanismo de autenticación de usuario similar cuando se deja sin supervisar y se debe proteger con bloqueos de tecla, contraseñas u otros controles cuando no está en uso. Si por alguna razón no funciona el bloqueo automático del equipo, el usuario deberá terminar sus sesiones activas. Se deben también cerrar las sesiones en los distintos sistemas, aplicaciones y/o servicios de redes cuando ya no se necesiten.
c) Se debe evitar el uso no autorizado de fotocopiadoras u otro tipo de tecnologías de reproducción (es decir, escáneres, cámaras digitales).

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. GLOSARIO

Perímetro de seguridad física: Corresponde a la zona cercada por los elementos físicos que, en su conjunto, permiten diferenciar las instalaciones del Servicio respecto del exterior, tales son paredes, puertas, accesos, salidas y entradas. Complementan a los elementos físicos los dispositivos de control de acceso magnético o biométrico, o un puesto manual de recepción.

Área segura: Son áreas que contienen información sensible o crítica y las instalaciones de procesamiento de información. Dentro de las áreas establecidas como seguras al interior de la institución, se encuentran definidas las salas de servidores o Datacenter, cuyo acceso es administrado por la sección de TI; depósitos documentales, cuyo acceso es administrado por cada una de los Departamentos o unidades y/o áreas al interior de cada una de ellas y la Oficina de Partes.

Área restringida: Son aquellas áreas cuyo acceso o movimiento dentro de las mismas está sujeto a ciertas restricciones o medidas de control especial por razones de seguridad. Se establecen con el propósito de resguardar los bienes, materiales, información y/o actividades que allí se encuentran o desarrollan. Dentro de las áreas establecidas como restringidas se encuentran las oficinas de directores, bodegas de almacenaje de activos y existencias y oficinas de la sección TI.

Equipos críticos: Son aquellos equipos que dan soporte a las operaciones críticas de la institución, tales como: servidores, dispositivos de comunicaciones, de seguridad y servicios básicos de apoyo.

8. CONTROL DEL DOCUMENTO

HISTORIA DEL DOCUMENTO	
Nombre del Documento:	Política de Seguridad Física y del Ambiente
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	09-08-2021	Modificación	Alcance; punto 4.6; firmas

FIRMAS

Claudio Henriquez
Claudio Henriquez (Nov 11, 2021 15:29 GMT-3)
Claudio Henriquez Rebolledo
Encargado de Unidad Continuidad Operativa TI

Andrés Carvajal
Andrés Carvajal (Nov 15, 2021 13:19 GMT-3)
Andrés Carvajal Rath
Director Departamento Recursos Financieros

Marco Ibacache O.
Marco Ibacache O. (Nov 18, 2021 14:18 GMT-3)
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 (Nov 11, 2021 15:13 GMT-3)
Enzo Marzán Oyarzún	Recursos Financieros	Enzo Marzán Oyarzún Enzo Marzán Oyarzún (Nov 10, 2021 11:49 GMT-3)
Javiera Osorio Estrada	Gestión y Desarrollo de las Personas	Javiera Osorio Estrada Javiera Osorio Estrada (Nov 11, 2021 14:38 GMT-3)
Julio Saavedra Rojas	Fiscalía y Asesoría Jurídica	
Constanza Sabater Orellana	Calidad Educativa	
Patricio Reyes Martínez	Unidad de Tecnologías de la Información	Patricio Reyes M. Patricio Reyes M. (Nov 10, 2021 08:41 GMT-3)

JUNJI_A.11_Política de Seguridad Física y del Ambiente_V1.2

Final Audit Report 2021-11-18

Created:	2021-11-10
By:	Patricio Reyes M. (PREYES@JUNJI.CL)
Status:	Signed
Transaction ID:	CBJCHBCAABAAgGuJSiWZ6VH2yv_ruCrWhd1R5-pERh7Y

"JUNJI_A.11_Política de Seguridad Física y del Ambiente_V1.2" History

Document created by Patricio Reyes M. (PREYES@JUNJI.CL)
2021-11-10 - 11:38:02 AM GMT- IP address: 190.22.27.177

Document e-signed by Patricio Reyes M. (PREYES@JUNJI.CL)
Signature Date: 2021-11-10 - 11:41:22 AM GMT - Time Source: server- IP address: 190.22.27.177

Document emailed to Enzo Marzán Oyarzún (emarzan@junji.cl) for signature
2021-11-10 - 11:41:25 AM GMT

Email viewed by Enzo Marzán Oyarzún (emarzan@junji.cl)
2021-11-10 - 2:37:37 PM GMT- IP address: 201.239.120.72

Document e-signed by Enzo Marzán Oyarzún (emarzan@junji.cl)
Signature Date: 2021-11-10 - 2:49:47 PM GMT - Time Source: server- IP address: 201.239.120.72

Document emailed to Julio Saavedra Rojas (jasaavedra@junji.cl) for signature
2021-11-10 - 2:49:49 PM GMT

Email viewed by Julio Saavedra Rojas (jasaavedra@junji.cl)
2021-11-11 - 1:50:49 PM GMT- IP address: 190.151.20.194

Document e-signed by Julio Saavedra Rojas (jasaavedra@junji.cl)
Signature Date: 2021-11-11 - 1:51:42 PM GMT - Time Source: server- IP address: 190.151.20.194

Document emailed to Javiera Osorio Estrada (jfosorio@junji.cl) for signature
2021-11-11 - 1:51:45 PM GMT

Email viewed by Javiera Osorio Estrada (jfosorio@junji.cl)
2021-11-11 - 2:02:51 PM GMT- IP address: 186.11.15.164

Adobe Sign

Document e-signed by Javiera Osorio Estrada (jfosorio@junji.cl)
Signature Date: 2021-11-11 - 5:38:40 PM GMT - Time Source: server- IP address: 186.156.158.251

Document emailed to Constanza Sabater (csabater@junji.cl) for signature
2021-11-11 - 5:38:41 PM GMT

Email viewed by Constanza Sabater (csabater@junji.cl)
2021-11-11 - 5:43:50 PM GMT- IP address: 200.111.176.225

Document e-signed by Constanza Sabater (csabater@junji.cl)
Signature Date: 2021-11-11 - 6:02:12 PM GMT - Time Source: server- IP address: 200.111.176.225

Document emailed to Cristian Cerda (ccerda@junji.cl) for signature
2021-11-11 - 6:02:15 PM GMT

Email viewed by Cristian Cerda (ccerda@junji.cl)
2021-11-11 - 6:13:37 PM GMT- IP address: 200.111.176.225

Document e-signed by Cristian Cerda (ccerda@junji.cl)
Signature Date: 2021-11-11 - 6:13:52 PM GMT - Time Source: server- IP address: 200.111.176.225

Document emailed to Claudio Henriquez (cahenriquez@junji.cl) for signature
2021-11-11 - 6:13:54 PM GMT

Email viewed by Claudio Henriquez (cahenriquez@junji.cl)
2021-11-11 - 6:27:46 PM GMT- IP address: 200.111.176.225

Document e-signed by Claudio Henriquez (cahenriquez@junji.cl)
Signature Date: 2021-11-11 - 6:29:14 PM GMT - Time Source: server- IP address: 200.111.176.225

Document emailed to Andrés Carvajal (arcarvajal@junji.cl) for signature
2021-11-11 - 6:29:17 PM GMT

Email viewed by Andrés Carvajal (arcarvajal@junji.cl)
2021-11-15 - 4:14:26 PM GMT- IP address: 200.111.176.225

Document e-signed by Andrés Carvajal (arcarvajal@junji.cl)
Signature Date: 2021-11-15 - 4:19:44 PM GMT - Time Source: server- IP address: 190.151.104.210

Document emailed to Marco Ibacache O. (mibacache@junji.cl) for signature
2021-11-15 - 4:19:47 PM GMT

Email viewed by Marco Ibacache O. (mibacache@junji.cl)
2021-11-18 - 5:18:01 PM GMT- IP address: 190.151.20.194

Document e-signed by Marco Ibacache O. (mibacache@junji.cl)
Signature Date: 2021-11-18 - 5:18:21 PM GMT - Time Source: server- IP address: 190.151.20.194

Adobe Sign

Agreement completed.

2021-11-18 - 5:18:21 PM GMT

Adobe Sign