MJC/FTO/PRC/CBC/NGG/AHM

APRUEBA POLÍTICA DE DESARROLLO SEGURO, AL INTERIOR DE LA SUPERINTENDENCIA DE EDUCACIÓN.

0746

RESOLUCIÓN EXENTA N°

SANTIAGO, 23 DIC 2019

Superintendencia de Educación
TOTALMENTE TRAMITADO

VISTO:

Lo dispuesto en el Decreto con Fuerza de Ley N° 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N° 19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que establece las Bases de los Procedimientos Administrativos que rigen los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado; En el Decreto con Fuerza de Ley N° 29, de 2004, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en la Ley N° 20.529, de 2011, del Ministerio de Educación, sobre el Sistema Nacional de Aseguramiento de la Calidad de la Educación parvulario, básica y media y su fiscalización; en el Decreto con Fuerza de Ley N° 5, de 2012, del Ministerio de Educación; en el Decreto de nombramiento del Superintendente de Educación, actualmente en trámite, del Ministerio de Educación; y en la Resolución Nº 6 y 7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que, la Ley Nº 20.529, crea la Superintendencia de Educación, en adelante la "Superintendencia", como un servicio público funcionalmente descentralizado y territorialmente desconcentrado, dotado de personalidad jurídica y patrimonio propio y que se relaciona con el Presidente de la República por intermedio del Ministerio de Educación.

2. Que, la Superintendencia tiene por objeto fiscalizar, de conformidad a la ley, que los sostenedores de establecimientos educacionales reconocidos oficialmente por el Estado se ajusten a las leyes, reglamentos e instrucciones que dicte la Superintendencia, en adelante "la normativa educacional". Asimismo, fiscalizará la legalidad del uso de los recursos por los sostenedores de los establecimientos subvencionados y que reciban aporte estatal y, respecto de los sostenedores de los establecimientos particulares pagados, fiscalizará la referida legalidad sólo en caso de denuncia. Además, proporcionará información, en el ámbito de su competencia, a las comunidades educativas y otros usuarios e interesados, y atenderá las denuncias y reclamos de éstos, aplicando las sanciones que en cada caso corresponda.

3. Que, mediante Resolución Exenta N° 0289, de fecha 24 de abril de 2019, se dispone la nueva organización interna de la División de Administración General, creándose el Departamento de Tecnología y Procesos.

4. Que, mediante Resolución Exenta N° 0698, de fecha 10 de diciembre de 2019, de este Servicio, se nombró al Comité de Seguridad de la Información Institucional, para

que, en función del marco legal y tecnológico, proponga a este Jefe de Servicio, un Sistema de Seguridad de la Información que se mantenga y mejore en el tiempo.

5. Que, en atención a lo ya mencionado se consideró necesario definir las directrices generales de seguridad de la información para el desarrollo, adquisición o mantención de los sistemas de información de esta Superintendencia, conforme al ciclo de vida del desarrollo de software y al marco metodológico aplicado por esta.

6. Que, finalmente resulta necesario aprobar mediante el presente acto administrativo la política de desarrollo seguro al interior de la Superintendencia de Educación.

RESUELVO:

1° APRUÉBASE, la política de desarrollo seguro al interior de la Superintendencia de Educación, cuyo texto es el siguiente:

Política de Desarrollo de Seguro

Tabla de Contenidos

REVISIONES DE LA POLÍTICA			
N° Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
Versión 0	20-12-2019	Versión inicial	Todas las páginas

ELABORADO POR	REVISADO POR	APROBADO POR
Mauricio Godoy Cisternas **Jefe Departamento** **Tecnología y Procesos**	**Claudio Borges Castillo** **Jefe División Administración General**	**Cristián O'Ryan Squella** **Superintendente de Educación**

Declaración institucional

En concordancia con la política general de seguridad de la información de la Superintendencia de Educación (SIE), gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, realizando todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, con el propósito de garantizar niveles adecuados de integridad, confidencialidad y disponibilidad de todos los activos de información relevantes para la institución.

En este contexto, la SIE se compromete a mantener políticas en el ámbito de la seguridad de la información, particularmente, en el área del desarrollo seguro de sistemas de información, con el fin de garantizar que estos, como herramientas de

apoyo a los procesos estratégicos de la institución, permitan brindar mejores servicios a la comunidad, con la debida continuidad operacional.

Objetivos

General

- Definir las directrices generales de seguridad de la información para el desarrollo, adquisición o mantención de los sistemas de información de la SIE, conforme al ciclo de vida del desarrollo de software y al marco metodológico aplicado por la SIE.

Específicos

- Establecer reglas para el desarrollo de software y sistemas dentro de la organización.
- Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información
- Definir una estructura y un marco de estándares y procedimientos en materias de desarrollo seguro de aplicaciones y sistemas de la Superintendencia de Educación.
- Establecer mecanismos de difusión de la presente política para el conocimiento de terceras pares y funcionarios de la SUPEREDUC.
- Monitorear el cumplimiento del procedimiento, norma y política de desarrollo, mediante el uso de herramientas diagnósticas y auditorías internas o externas, a intervalos regulares y de acuerdo a la disponibilidad de recursos en la institución.
- Aplicar mejoras y acciones correctivas, relacionadas con el desarrollo de sistemas para contribuir al sistema de gestión de seguridad de la información.
- Establecer la inclusión de controles de seguridad y validación de datos en la adquisición y desarrollo de sistemas de información, para generar un servicio, arquitectura, software y sistema seguro.
- Definir y documentar las normas, riesgos y procedimientos que se aplicarán e identificarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Establecer los métodos de protección de la información crítica o sensible.

Alcance

El ámbito de aplicación de esta política, corresponde a los dominios y controles de seguridad de la información detallados a continuación:

- A.12.01.04 Separación de los ambientes de desarrollo, prueba y operacionales.
- A.12.05.01 Instalación del software en sistemas operacionales.
- A.14.01.01 Análisis y especificación de los requisitos de seguridad de la información.
- A.14.01.02 Aseguramiento de servicios de aplicación en redes públicas.
- A.14.02.01 Política de desarrollo seguro.
- A.14.02.02 Procedimientos de control de cambios.
- A.14.02.06 Entorno de desarrollo seguro.
- A.14.02.08 Pruebas de seguridad del sistema.
- A.14.02.09 Pruebas de aprobación del sistema.

Su alcance aplica a todos los sistemas de información, tanto desarrollo propio o de terceros, y a todos los sistemas operativos y/o software básico, que integren cualquiera de los ambientes administrados por la SIE, en donde residan los desarrollos antes mencionados.
La aplicación completa o parcial de la presente política, queda sujeta a la disponibilidad de capacidades internas, a los recursos tecnológicos, presupuesto y, asimismo, a la oportunidad y los plazos que determinen las necesidades o exigencias institucionales, en el ámbito de desarrollo o adquisición de sistemas.

Referencias normativas:

- Procedimiento de Desarrollo Seguro vigente.
- Política General de Seguridad de la Información de la Superintendencia de Educación vigente.
- Política de seguridad para la gestión de cambios a los servicios del proveedor de la Superintendencia de Educación vigente.
- Política de seguridad que regula la relación con proveedores de bienes y/o servicios de la Superintendencia de Educación vigente.
- Política de Gestión de Incidentes de Seguridad de la información de la Superintendencia de Educación vigente.
- Guía técnica - Lineamientos para Desarrollo de Software, diciembre de 2018, Gobierno Digital, Ministerio Secretaria General de la Presidencia.
- Norma Chilena NCh-ISO 27001/2013 tecnología de la información-técnicas de seguridad-sistemas de gestión de la seguridad de la información.
- Instructivo Presidencial N°8, de 23 de octubre de 2018, que imparte instrucciones en materias de Ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos del Estado.

Definiciones:

Concepto	Descripción
Sistema de Información	Corresponden a todos los sistemas operativos, infraestructura, aplicaciones, y servicios de la SUPEREDUC y que permiten administrar, recolectar, recuperar, procesar y almacenar y distribuir información relevante para los procesos que lidera la Superintendencia de Educación. EJ: sistema SIAC, SIPE, Rendición de Cuentas, entre otros.
Unidades de negocio	Intendencia Parvularia, Divisiones de Fiscalización, Fiscalía, Comunicaciones y Denuncias y Administración General y todas sus unidades y áreas dependientes.
Entornos o ambientes	Infraestructura tecnológica disponible para alojar y soportar el funcionamiento de sistemas de información, para efectos de su desarrollo, pruebas u operación, en términos de servidores, sistemas operativos, compiladores, bases de datos, balanceadores de carga, "web application firewall" (WAF), entre otros.
Evaluación de Riesgos	Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la Institución.
Seguridad de los activos de Información	Consiste en proteger, resguardar y asegurar la disponibilidad, privacidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento, a efecto de garantizar la continuidad operacional de la institución.
Ambiente de Producción	Plataforma tecnológica dispuesta para alojar las aplicaciones que utilizan los usuarios para realizar sus funciones.
Ambiente de Desarrollo	Plataforma donde se instalarán los componentes necesarios para el desarrollo de aplicaciones o sistemas de información. Corresponde también a la infraestructura necesaria para instalar un software propietario, el cual es personalizado para su posterior uso en la SIE.
Ambiente de Pruebas o Testing o QA (Quality Assurance)	Plataforma donde están disponibles los sistemas de información recientemente desarrollados o personalizados, para su revisión por parte de los usuarios finales, desde un

Concepto	Descripción
	punto de vista funcional, y por el Departamento de Tecnologías y Procesos, para pruebas de estrés, rendimiento y seguridad.

Roles y Responsabilidades:

Rol	Responsabilidad
Comité Directivo de Seguridad de la Información	a) Supervisar la implementación de la presente política. b) Definir y elaborar la nómina de sistemas de información clasificados como "críticos" para la Institución. Los sistemas de información, clasificados como tal, podrán corresponder a desarrollos a la medida o a licencias de aplicaciones.
Encargado/a de Seguridad de la Información	a) Proponer, desarrollar y actualizar la presente política al interior de la institución, coordinar su implementación y evaluación, velando por su correcta aplicación. b) En conjunto con cada dueño o responsable de sistemas de información, es responsable de definir el nivel de criticidad de los sistemas de información y de identificar los controles de seguridad a aplicar para su debido resguardo. c) 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. d) Verificar el cumplimiento de los procedimientos y controles de seguridad establecidos para la construcción, mantención y adquisición de sistemas de información.
Jefatura Departamento Tecnologías y Procesos	a) Establecer los procedimientos, mejores prácticas, estándares y normas en el ámbito de desarrollo de sistemas y seguridad de la información (integridad y confidencialidad) y su soporte tecnológico, velando por el cumplimiento de la normativa vigente y vinculante. b) En conjunto con el/la Encargado/a de Seguridad de la Información, son los responsables de la seguridad de los sistemas de información (seguridad informática) de la SIE.
Encargado/a Unidad Desarrollo	a) Establecer las mejores prácticas, estándares, procedimientos y controles que permitan asegurar que, dentro del ciclo de desarrollo de un software, se apliquen los controles o requisitos necesarios para la seguridad de los sistemas de información en cada una de sus etapas. b) Promover e incorporar el cumplimiento de la política de seguridad enunciada en el presente documento.
Encargado/a Unidad Infraestructura Operacional	a) Implementar, administrar, promover y disponer los mecanismos de seguridad nativos, propios de las plataformas e infraestructura, con el fin que estos sean utilizados por las aplicaciones que serán desarrolladas para operar.
Encargado/a Unidad de Proyectos	a) Gestionar de manera preventiva los riesgos institucionales asociados a la implementación de tecnologías de la información y comunicaciones (TIC). b) Definir y proponer estándares o normas orientadas a la definición, especificación y planificación de soluciones de negocios. c) De manera conjunta con el Encargado de Seguridad de la Información, es responsable de especificar, verificar y validar los requerimientos de seguridad que deben cumplir

Rol	Responsabilidad
	los paquetes de software ofertados en el mercado, independiente de cómo se realiza la adquisición por parte de la SIE. d) Promover e incorporar el cumplimiento de la política de seguridad enunciada en el presente documento.

Directrices

Lineamientos generales
Como marco general para la normativa de desarrollo seguro, los objetivos de seguridad a cumplir serán los siguientes:

a) La seguridad debe estar incorporada en el ciclo de desarrollo de sistemas, resguardando los activos de información que resulten sensibles: bases de datos personales, información estratégica, acuerdos de confidencialidad, documentación e información de control de proyectos.
b) Se deberán implementar procedimientos para controlar la instalación de software en sistemas operacionales.
c) En cuanto a los requisitos asociados a la seguridad de la información, estos deberán ser incluidos y aplicados en el desarrollo de nuevos sistemas para la SIE o mejoras de sistemas ya existentes.
d) La información de los servicios de aplicación compartidos a través de redes públicas, deberán ser protegidos contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.
e) Establecer, en el marco del sistema de seguridad de la información, un procedimiento para generar y almacenar documentación en el desarrollo y mantención de sistemas: requerimientos, diseños, modelos y cualquier producto que se encuentre relacionado.
f) Se deberán establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.
g) En el ciclo de vida de desarrollo, se deberán aplicar procedimientos formales de control de cambios.
h) La institución deberá establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
i) Se deberán realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
j) Se deberán establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.
k) Los entornos de desarrollo, pruebas y operacionales deberán permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.

Requisitos de seguridad en los sistemas de información

Para el diseño e implantación de los sistemas de información que sustentan los procesos de negocio de la SIE, los requisitos de seguridad deberán ser identificados y consensuados previo a su desarrollo y/o implantación. Para ello, todos los requisitos de seguridad deberán ser identificados en la fase de levantamiento de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso de implementación de un sistema de información. Adicionalmente, se deberá trabajar estrechamente con las unidades de negocio para desarrollar sistemas de información seguros, incorporando desde un comienzo requisitos de seguridad de la información en los proyectos.

En este sentido, para los siguientes ámbitos, se deberán cumplir los siguientes objetivos de seguridad específicos:

Análisis y especificación de requisitos de seguridad

- Los requisitos de seguridad de la información se ponderarán dentro de la etapa de análisis del ciclo de desarrollo de sistemas de información, es decir, previo a su fase de desarrollo.
- Los requisitos de seguridad deberán considerar valoraciones del impacto en el negocio de posibles fallas de seguridad (daño potencial).

Protección de servicios de aplicación en redes públicas

- Los sistemas utilizados a través de redes públicas, deberán cumplir con controles de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información y acceso a ella.
- Se deberán encriptar las comunicaciones de los servicios expuestos a redes públicas.
- Se utilizarán métodos robustos de autenticación para aquellas aplicaciones críticas del negocio, expuestas a redes públicas.
- Los sistemas deberán incluir un mecanismo de cifrado de datos, que se transporten entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.
- Los sistemas deberán permitir la implementación de certificados digitales, tanto en software como en hardware.
- Los sistemas deberán implementar el mecanismo de firma o validación o autorización de documentos mediante firma mecánica o digital.
- Los sistemas deberán incluir uso de criptografía para transacciones y/o campos sensibles, según lo indiquen las definiciones vigentes y las necesidades específicas del negocio.
- Los sistemas deberán funcionar sobre protocolos SSL, es decir, certificados internos de la entidad, cuando los sistemas de información sean internas y certificados validos públicamente, cuando los sistemas de información estén expuestas a internet.
- Se implementarán controles para evitar la pérdida o duplicación de información de las transacciones de los sistemas.

Ambiente de desarrollo

- Efectuar una evaluación de riesgos de seguridad de la información en los entornos y procesos de desarrollo, así como en las tecnologías utilizadas, con el objetivo de determinar medidas o controles de seguridad, según corresponda.

Control de versiones

- Se deberán aplicar procedimientos de control de cambios y versiones a toda la documentación, archivos ejecutables, códigos fuente y librerías de software de los sistemas construidos, script de bases de datos, así como la documentación de paquetes de software adquiridos.
- Se deberá mantener un registro actualizado de todos los sistemas en explotación, con datos respecto a su versión, fecha de última compilación, responsable(s) de su mantención y soporte, entre otros datos relevantes.

Control de cambios a sistemas

- Durante las fases de construcción y mantenimiento, se supervisará y controlarán todos los cambios realizados a los sistemas de información.

Pruebas de seguridad

- Los requisitos para la seguridad de un sistema de información deberán ser evaluados como una funcionalidad más del software, debiendo para ello implementarse un plan de pruebas documentado, incluyendo pruebas a softwares provistos por terceros, mediante labores de desarrollo de software, adquisición de licencias o de software como servicio.

Pruebas de aceptación

- El proceso de incorporación de nuevas aplicaciones, actualizaciones o nuevas versiones de sistemas de información, deberá estar sujeto a un proceso de aceptación, donde se realicen pruebas funcionales y de seguridad planificadas. Los entornos de pruebas deberán ser distintos a los entornos de operación, con el objetivo de evitar fallas en sistemas reales.

Separación de Ambientes

- Durante la implementación de nuevos sistemas de información, actualizaciones o mejoras a sistemas existentes, se deberán habilitar ambientes (entornos) diferenciados, para efectos de desarrollo, pruebas y operación, los cuales deberán permanecer separados, con el objetivo de reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.

Evaluación y difusión

La presente política será evaluada por el Superintendente de Educación al menos una vez al año o, bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar su continua idoneidad, eficiencia y efectividad.

Una vez que el documento entre en vigencia el/la Encargado/a de Seguridad de la Información y Ciberseguridad deberá difundir al personal y externos considerado en el alcance mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrán ser página web institucional, intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

Revisión del cumplimiento de la Política:

Con una periodicidad concordante a la de la evaluación definida en el punto anterior, y a través de auditorías, ya sean internas o externas, y en tanto los recursos institucionales se encuentren disponibles para ello, se revisará el cumplimiento de la presente política con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento o mejora de la misma.

Aceptación

Todos los usuarios de la SIE, sean planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, deben aceptar esta política y procedimientos relacionados.
Para el caso de terceros y por el solo hecho de participar en algún proceso de compras del servicio, el oferente debe dar cumplimiento a la política y procedimientos vigentes de seguridad de la información de la SIE, publicados en el sitio web www.supereduc.cl y sus correspondientes modificaciones, las cuales se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

Sanciones

El incumplimiento o violación a esta política, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios/as de la SIE, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

Excepciones

La presente Política, y las Políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el/la Encargado/a de Seguridad de la Información y Ciberseguridad y debidamente autorizados por la Jefatura de Gabinete.

3° ESTABLÉZCASE, que la política que por medio de la presente Resolución Exenta se aprueba, comenzará a regir de manera inmediata una vez que esta haya quedado totalmente tramitada.

4° PUBLÍQUESE, la presente Resolución Exenta en la intranet institucional.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

CRISTIÁN O'RYAN SQUELLA
SUPERINTENDENTE DE EDUCACIÓN

Distribución:
1. Gabinete
2. División de Fiscalización
3. División de Fiscalía
4. División de Administración General
5. División de Comunicación y Denuncias
6. Departamento de Auditoría
7. Departamento de Gestión Institucional
8. Departamento de Tecnologías de la Información
9. Departamento de Gestión y Desarrollo de Personas
10. Unidad de Desarrollo de Personas
11. Unidad de Actos y Contratos- Fiscalía
12. Oficina de Partes.

Superintendencia de Educación / Gobierno de Chile	**Política de Desarrollo Seguro**			
	Fecha revisión del documento	20-12-2019	Páginas	1 de 7
			Versión	0.0
	Nivel de Confidencialidad	Uso Interno	Código	POL-DAG-DTP-01
	Departamento de Tecnología y Procesos			

Política de Desarrollo de Seguro

Tabla de Contenidos

REVISIONES DE LA POLÍTICA

Nº Versión	Fecha	Motivo de la revisión	Paginas elaboradas o modificadas
Versión 0	20-12-2019	Versión inicial	Todas las páginas

ELABORADO POR	REVISADO POR	APROBADO POR
Mauricio Godoy Cisternas **Jefe Departamento** **Tecnología y Procesos**	**Claudio Borges Castillo** **Jefe División Administración General**	**Cristián O'Ryan Squella** **Superintendente de Educación**

SUPERINTENDENCIA DE EDUCACIÓN JEFE T. I.

1 Declaración institucional

En concordancia con la política general de seguridad de la información de la Superintendencia de Educación (SIE), gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, realizando todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, con el propósito de garantizar niveles adecuados de integridad, confidencialidad y disponibilidad de todos los activos de información relevantes para la institución.

En este contexto, la SIE se compromete a mantener políticas en el ámbito de la seguridad de la información, particularmente, en el área del desarrollo seguro de sistemas de información, con el fin de garantizar que estos, como herramientas de apoyo a los procesos estratégicos de la institución, permitan brindar mejores servicios a la comunidad, con la debida continuidad operacional.

2 Objetivos

2.1 General

- Definir las directrices generales de seguridad de la información para el desarrollo, adquisición o mantención de los sistemas de información de la SIE, conforme al ciclo de vida del desarrollo de software y al marco metodológico aplicado por la SIE.

2.2 Específicos

- Establecer reglas para el desarrollo de software y sistemas dentro de la organización.
- Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información
- Definir una estructura y un marco de estándares y procedimientos en materias de desarrollo seguro de aplicaciones y sistemas de la Superintendencia de Educación.
- Establecer mecanismos de difusión de la presente política para el conocimiento de terceras pares y funcionarios de la SUPEREDUC.
- Monitorear el cumplimiento del procedimiento, norma y política de desarrollo, mediante el uso de herramientas diagnósticas y auditorías internas o externas, a intervalos regulares y de acuerdo a la disponibilidad de recursos en la institución.
- Aplicar mejoras y acciones correctivas, relacionadas con el desarrollo de sistemas para contribuir al sistema de gestión de seguridad de la información.
- Establecer la inclusión de controles de seguridad y validación de datos en la adquisición y desarrollo de sistemas de información, para generar un servicio, arquitectura, software y sistema seguro.
- Definir y documentar las normas, riesgos y procedimientos que se aplicarán e identificarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Establecer los métodos de protección de la información crítica o sensible.

3 Alcance

El ámbito de aplicación de esta política, corresponde a los dominios y controles de seguridad de la información detallados a continuación:

- A.12.01.04 Separación de los ambientes de desarrollo, prueba y operacionales.
- A.12.05.01 Instalación del software en sistemas operacionales.
- A.14.01.01 Análisis y especificación de los requisitos de seguridad de la información.
- A.14.01.02 Aseguramiento de servicios de aplicación en redes públicas.
- A.14.02.01 Política de desarrollo seguro.
- A.14.02.02 Procedimientos de control de cambios.
- A.14.02.06 Entorno de desarrollo seguro.

- A.14.02.08 Pruebas de seguridad del sistema.
- A.14.02.09 Pruebas de aprobación del sistema.

Su alcance aplica a todos los sistemas de información, tanto desarrollo propio o de terceros, y a todos los sistemas operativos y/o software básico, que integren cualquiera de los ambientes administrados por la SIE, en donde residan los desarrollos antes mencionados.

La aplicación completa o parcial de la presente política, queda sujeta a la disponibilidad de capacidades internas, a los recursos tecnológicos, presupuesto y, asimismo, a la oportunidad y los plazos que determinen las necesidades o exigencias institucionales, en el ámbito de desarrollo o adquisición de sistemas.

4 Referencias normativas:

- Procedimiento de Desarrollo Seguro vigente.
- Política General de Seguridad de la Información de la Superintendencia de Educación vigente.
- Política de seguridad para la gestión de cambios a los servicios del proveedor de la Superintendencia de Educación vigente.
- Política de seguridad que regula la relación con proveedores de bienes y/o servicios de la Superintendencia de Educación vigente.
- Política de Gestión de Incidentes de Seguridad de la información de la Superintendencia de Educación vigente.
- Guía técnica - Lineamientos para Desarrollo de Software, diciembre de 2018, Gobierno Digital, Ministerio Secretaria General de la Presidencia.
- Norma Chilena NCh-ISO 27001/2013 tecnología de la información-técnicas de seguridad-sistemas de gestión de la seguridad de la información.
- Instructivo Presidencial N°8, de 23 de octubre de 2018, que imparte instrucciones en materias de Ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos del Estado.

5 Definiciones:

Concepto	Descripción
Sistema de Información	Corresponden a todos los sistemas operativos, infraestructura, aplicaciones, y servicios de la SUPEREDUC y que permiten administrar, recolectar, recuperar, procesar y almacenar y distribuir información relevante para los procesos que lidera la Superintendencia de Educación. EJ: sistema SIAC, SIPE, Rendición de Cuentas, entre otros.
Unidades de negocio	Intendencia Parvularia, Divisiones de Fiscalización, Fiscalía, Comunicaciones y Denuncias y Administración General y todas sus unidades y áreas dependientes.
Entornos o ambientes	Infraestructura tecnológica disponible para alojar y soportar el funcionamiento de sistemas de información, para efectos de su desarrollo, pruebas u operación, en términos de servidores, sistemas operativos, compiladores, bases de datos, balanceadores de carga, "web application firewall" (WAF), entre otros.
Evaluación de Riesgos	Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la Institución.
Seguridad de los activos de Información	Consiste en proteger, resguardar y asegurar la disponibilidad, privacidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento, a efecto de garantizar la continuidad operacional de la institución.
Ambiente de Producción	Plataforma tecnológica dispuesta para alojar las aplicaciones que utilizan los usuarios para realizar sus funciones.

Concepto	Descripción
Ambiente de Desarrollo	Plataforma donde se instalarán los componentes necesarios para el desarrollo de aplicaciones o sistemas de información. Corresponde también a la infraestructura necesaria para instalar un software propietario, el cual es personalizado para su posterior uso en la SIE.
Ambiente de Pruebas o Testing o QA (Quality Assurance)	Plataforma donde están disponibles los sistemas de información recientemente desarrollados o personalizados, para su revisión por parte de los usuarios finales, desde un punto de vista funcional, y por el Departamento de Tecnologías y Procesos, para pruebas de estrés, rendimiento y seguridad.

6 Roles y Responsabilidades:

Rol	Responsabilidad
Comité Directivo de Seguridad de la Información	a) Supervisar la implementación de la presente política. b) Definir y elaborar la nómina de sistemas de información clasificados como "críticos" para la Institución. Los sistemas de información, clasificados como tal, podrán corresponder a desarrollos a la medida o a licencias de aplicaciones.
Encargado/a de Seguridad de la Información	a) Proponer, desarrollar y actualizar la presente política al interior de la institución, coordinar su implementación y evaluación, velando por su correcta aplicación. b) En conjunto con cada dueño o responsable de sistemas de información, es responsable de definir el nivel de criticidad de los sistemas de información y de identificar los controles de seguridad a aplicar para su debido resguardo. c) 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. d) Verificar el cumplimiento de los procedimientos y controles de seguridad establecidos para la construcción, mantención y adquisición de sistemas de información.
Jefatura Departamento Tecnologías y Procesos	a) Establecer los procedimientos, mejores prácticas, estándares y normas en el ámbito de desarrollo de sistemas y seguridad de la información (integridad y confidencialidad) y su soporte tecnológico, velando por el cumplimiento de la normativa vigente y vinculante. b) En conjunto con el/la Encargado/a de Seguridad de la Información, son los responsables de la seguridad de los sistemas de información (seguridad informática) de la SIE.
Encargado/a Unidad Desarrollo	a) Establecer las mejores prácticas, estándares, procedimientos y controles que permitan asegurar que, dentro del ciclo de desarrollo de un software, se apliquen los controles o requisitos necesarios para la seguridad de los sistemas de información en cada una de sus etapas. b) Promover e incorporar el cumplimiento de la política de seguridad enunciada en el presente documento.
Encargado/a Unidad Infraestructura Operacional	a) Implementar, administrar, promover y disponer los mecanismos de seguridad nativos, propios de las plataformas e infraestructura, con el fin que estos sean utilizados por las aplicaciones que serán desarrolladas para operar.
Encargado/a Unidad de Proyectos	a) Gestionar de manera preventiva los riesgos institucionales asociados a la implementación de tecnologías de la información y comunicaciones (TIC). b) Definir y proponer estándares o normas orientadas a la definición, especificación y planificación de soluciones de negocios.

Rol	Responsabilidad
	c) De manera conjunta con el Encargado de Seguridad de la Información, es responsable de especificar, verificar y validar los requerimientos de seguridad que deben cumplir los paquetes de software ofertados en el mercado, independiente de cómo se realiza la adquisición por parte de la SIE. d) Promover e incorporar el cumplimiento de la política de seguridad enunciada en el presente documento.

7 Directrices

7.1 Lineamientos generales

Como marco general para la normativa de desarrollo seguro, los objetivos de seguridad a cumplir serán los siguientes:

a) La seguridad debe estar incorporada en el ciclo de desarrollo de sistemas, resguardando los activos de información que resulten sensibles: bases de datos personales, información estratégica, acuerdos de confidencialidad, documentación e información de control de proyectos.
b) Se deberán implementar procedimientos para controlar la instalación de software en sistemas operacionales.
c) En cuanto a los requisitos asociados a la seguridad de la información, estos deberán ser incluidos y aplicados en el desarrollo de nuevos sistemas para la SIE o mejoras de sistemas ya existentes.
d) La información de los servicios de aplicación compartidos a través de redes públicas, deberán ser protegidos contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.
e) Establecer, en el marco del sistema de seguridad de la información, un procedimiento para generar y almacenar documentación en el desarrollo y mantención de sistemas: requerimientos, diseños, modelos y cualquier producto que se encuentre relacionado.
f) Se deberán establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.
g) En el ciclo de vida de desarrollo, se deberán aplicar procedimientos formales de control de cambios.
h) La institución deberá establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
i) Se deberán realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
j) Se deberán establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.
k) Los entornos de desarrollo, pruebas y operacionales deberán permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.

7.2 Requisitos de seguridad en los sistemas de información

Para el diseño e implantación de los sistemas de información que sustentan los procesos de negocio de la SIE, los requisitos de seguridad deberán ser identificados y consensuados previo a su desarrollo y/o implantación. Para ello, todos los requisitos de seguridad deberán ser identificados en la fase de levantamiento de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso de implementación de un sistema de información. Adicionalmente, se deberá trabajar estrechamente con las unidades de negocio para desarrollar sistemas de información seguros, incorporando desde un comienzo requisitos de seguridad de la información en los proyectos.

En este sentido, para los siguientes ámbitos, se deberán cumplir los siguientes objetivos de seguridad específicos:

7.2.1 Análisis y especificación de requisitos de seguridad

- Los requisitos de seguridad de la información se ponderarán dentro de la etapa de análisis del ciclo de desarrollo de sistemas de información, es decir, previo a su fase de desarrollo.

- Los requisitos de seguridad deberán considerar valoraciones del impacto en el negocio de posibles fallas de seguridad (daño potencial).

7.2.2 Protección de servicios de aplicación en redes públicas

- Los sistemas utilizados a través de redes públicas, deberán cumplir con controles de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información y acceso a ella.
- Se deberán encriptar las comunicaciones de los servicios expuestos a redes públicas.
- Se utilizarán métodos robustos de autenticación para aquellas aplicaciones críticas del negocio, expuestas a redes públicas.
- Los sistemas deberán incluir un mecanismo de cifrado de datos, que se transporten entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.
- Los sistemas deberán permitir la implementación de certificados digitales, tanto en software como en hardware.
- Los sistemas deberán implementar el mecanismo de firma o validación o autorización de documentos mediante firma mecánica o digital.
- Los sistemas deberán incluir uso de criptografía para transacciones y/o campos sensibles, según lo indiquen las definiciones vigentes y las necesidades específicas del negocio.
- Los sistemas deberán funcionar sobre protocolos SSL, es decir, certificados internos de la entidad, cuando los sistemas de información sean internas y certificados validos públicamente, cuando los sistemas de información estén expuestas a internet.
- Se implementarán controles para evitar la pérdida o duplicación de información de las transacciones de los sistemas.

7.2.3 Ambiente de desarrollo

- Efectuar una evaluación de riesgos de seguridad de la información en los entornos y procesos de desarrollo, así como en las tecnologías utilizadas, con el objetivo de determinar medidas o controles de seguridad, según corresponda.

7.2.4 Control de versiones

- Se deberán aplicar procedimientos de control de cambios y versiones a toda la documentación, archivos ejecutables, códigos fuente y librerías de software de los sistemas construidos, script de bases de datos, así como la documentación de paquetes de software adquiridos.
- Se deberá mantener un registro actualizado de todos los sistemas en explotación, con datos respecto a su versión, fecha de última compilación, responsable(s) de su mantención y soporte, entre otros datos relevantes.

7.2.5 Control de cambios a sistemas

- Durante las fases de construcción y mantenimiento, se supervisará y controlarán todos los cambios realizados a los sistemas de información.

7.2.6 Pruebas de seguridad

- Los requisitos para la seguridad de un sistema de información deberán ser evaluados como una funcionalidad más del software, debiendo para ello implementarse un plan de pruebas documentado, incluyendo pruebas a softwares provistos por terceros, mediante labores de desarrollo de software, adquisición de licencias o de software como servicio.

7.2.7 Pruebas de aceptación

- El proceso de incorporación de nuevas aplicaciones, actualizaciones o nuevas versiones de sistemas de información, deberá estar sujeto a un proceso de aceptación, donde se realicen pruebas funcionales y de seguridad planificadas. Los entornos de pruebas deberán ser distintos a los entornos de operación, con el objetivo de evitar fallas en sistemas reales.

7.2.8 Separación de Ambientes

- Durante la implementación de nuevos sistemas de información, actualizaciones o mejoras a sistemas existentes, se deberán habilitar ambientes (entornos) diferenciados, para efectos de desarrollo, pruebas y operación, los cuales deberán permanecer separados, con el objetivo de reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.

8 Evaluación y difusión

La presente política será evaluada por el Superintendente de Educación al menos una vez al año o, bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar su continua idoneidad, eficiencia y efectividad.

Una vez que el documento entre en vigencia el/la Encargado/a de Seguridad de la Información y Ciberseguridad deberá difundir al personal y externos considerado en el alcance mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrán ser página web institucional, intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

9 Revisión del cumplimiento de la Política:

Con una periodicidad concordante a la de la evaluación definida en el punto anterior, y a través de auditorías, ya sean internas o externas, y en tanto los recursos institucionales se encuentren disponibles para ello, se revisará el cumplimiento de la presente política con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento o mejora de la misma.

10 Aceptación

Todos los usuarios de la SIE, sean planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, deben aceptar esta política y procedimientos relacionados.
Para el caso de terceros y por el solo hecho de participar en algún proceso de compras del servicio, el oferente debe dar cumplimiento a la política y procedimientos vigentes de seguridad de la información de la SIE, publicados en el sitio web www.supereduc.cl y sus correspondientes modificaciones, las cuales se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

11 Sanciones

El incumplimiento o violación a esta política, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios/as de la SIE, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

12 Excepciones

La presente Política, y las Políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el/la Encargado/a de Seguridad de la Información y Ciberseguridad y debidamente autorizados por la Jefatura de Gabinete.