

POLITICAS DE SEGURIDAD Y DESARROLLO SEGURO

(OCD) Official Cybersecurity Document

Version 0.4

Identificación de Documento

|  |  |
| --- | --- |
| **Identificación** | DOC-OFD-0102 |
| **Proyecto** | Trabajo Seguridad |
| **Versión** | 1-2 |

|  |  |
| --- | --- |
| **Documento mantenido por** | Jaime Malhue / Liza Molina |
| **Fecha de última revisión** | 09 de noviembre de 2024 |
| **Fecha de próxima revisión** | 10 de noviembre de 2024 |

|  |  |
| --- | --- |
| **Documento aprobado por** |  |
| **Fecha de última aprobación** |  |

Historia de cambios

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Descripción** | **Autor** |
| 29 de septiembre | 0.1 | Implementación de 1 a 3 | Liza Molina |
| 01 de octubre | 0.2 | Implementación de 3 a 5 | Jaime Malhue |
| 08 de octubre | 0.3 | Implementación de 6 a 7 | Jaime Malhue |
| 10 de octubre | 0.4 | Implementación de 8 a 9 | Liza Molina |

Tabla de contenido

[Introducción 3](#_Toc116324021)

[Contexto del Problema 3](#_Toc116324022)

[1 Alcance 3](#_Toc116324023)

[2 Marco de referencias 3](#_Toc116324024)

[3 Definiciones destacadas utilizadas 4](#_Toc116324025)

[4 Consideraciones Generales 5](#_Toc116324026)

[5 Desarrollo de Terceros 5](#_Toc116324027)

[6 Desarrollo Interno 6](#_Toc116324028)

[6.1 Política de Desarrollo Seguro 6](#_Toc116324029)

[6.2 Control de Acceso al Código Fuente de los Programas 6](#_Toc116324030)

[6.3 Protección de Servicios de Aplicación en Redes Publicas 7](#_Toc116324031)

[6.4 Entorno de Desarrollo Seguro 7](#_Toc116324032)

[6.5 Capacitaciones sobre Vulnerabilidades 8](#_Toc116324033)

[6.6 PREVENCIÓN, REACCIÓN Y MITIGACIÓN DE VIOLACIONES DE SEGURIDAD 8](#_Toc116324034)

[Copias de seguridad 8](#_Toc116324035)

[Pruebas 8](#_Toc116324036)

[6.7 Separación de Entornos de Desarrollo, Prueba y Operacionales 9](#_Toc116324037)

[6.8 Incidentes 9](#_Toc116324038)

[6.9 Seguridad del Sistema 9](#_Toc116324039)

[6.10 Pruebas de Aprobación del Sistema 10](#_Toc116324040)

[6.11 Principios de Ingeniería Segura del Sistema 10](#_Toc116324041)

[7 Post Implementación y marcha blanca 10](#_Toc116324042)

[7.1 Planifique su post implementación 10](#_Toc116324043)

[8 Periodo Revisión del Documento 11](#_Toc116324044)

[9 Periodo Revisión del Documento 11](#_Toc116324045)

Introducción

## Contexto del Problema

El propósito de esta política de desarrollo seguro es garantizar la seguridad de la información como parte integral del ciclo de vida de los sistemas de información institucionales, el cual influye en las fases de adquisición, desarrollo y mantenimiento de software y sistemas. Esta política considera un conjunto de reglas y prácticas orientadas a proteger el uso inapropiado de la información, por parte de los funcionarios de la Institución o de personal externo a ella.

# Alcance

La presente política de desarrollo seguro se dicta en cumplimiento de las disposiciones legales vigentes, con el objetivo de gestionar adecuadamente la seguridad de la información y los sistemas informáticos de la Institución. La presenta política de seguridad de la información aplica tanto a funcionarios de la institución como a los terceros que prestan apoyo a estos incluyendo el administrador de redes. Además de lo anterior el procedimiento abarca a todos los activos de información que requiera el equipo de desarrollo, incluyendo el Datacenter.

# Marco de referencias

A continuación, se listan las referencias a otros documentos:

¿Qué es ISO 27000?

La ISO 27000 es una familia de normas que define cómo implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa, creada por la Organización Internacional de Normalización (ISO).

* Norma Chilena ISO 27001:2013 Tecnología de la información - Técnicas de seguridad – Sistemas de gestión de la seguridad de la información.

Norma que define cómo planificar y verificar un SGSI. Tras un análisis de riesgo, planifica acciones que mitigarán estos riesgos. Sus procedimientos abarcan rubros legales, físicos y técnicos.

* Norma Chilena ISO 27002:2013 Tecnologías de la Información – Técnicas de Seguridad - Código de prácticas para los controles de seguridad de la información.

Es un código de 12 buenas prácticas para la gestión de seguridad de la información, destacando la creación de:

Plan de análisis de riesgo.

Política de seguridad detallada.

Departamento de gestión de activos.

Administración de operación y puntos de acceso.

Departamento de sistemas y mantenimiento de información.

Sistema de control de incidentes.

* Trabajo con principios OWASP.

# Definiciones destacadas utilizadas

* **DESARROLLO SEGURO:** Requisito para generar un servicio, arquitectura, software y sistema seguro, desde la perspectiva del resguardo de la información.
* **VULNERABILIDADES:** se refiere a la condición de debilidad o fragilidad que se encuentra presente en el activo identificado. Generalmente se traduce en una debilidad o ausencia de control, que posibilita la ocurrencia de un incidente y que puede afectar a uno o más activos de la información.
* **ENTORNO DE DESARROLLO:** Corresponde a los funcionarios institucionales o personal externo que forma parte del grupo a cargo de analizar y programar las funcionalidades de proyectos de desarrollo software y sistemas.
* **POLITICAS:** Las Políticas de Operación son guías de acción que definen los límites y parámetros necesarios para ejecutar los procesos y actividades en cumplimiento de la función, planes, programas, proyectos y políticas de la administración del riesgo, previamente definidos por la organización dentro de carabineros de chile.
* **CODIGO FUENTE:** En informática, se denomina código fuente al conjunto de líneas de texto que expresan, en un lenguaje de programación determinado, los pasos que debe seguir el computador para la correcta ejecución de un programa específico.
* **INTEGRIDAD:** La propiedad de salvaguardar la exactitud y complejidad de la información. (Norma ISO27000:2014)
* **REDES:** Entendemos como red de datos aquella infraestructura que ha sido creada con el objetivo de transmitir datos e información de cualquier tipo desde un punto a otro. Esto también se llama red informática, ya que está compuesta de nodos conectados entre sí, bien mediante cable o directamente por ondas electromagnéticas. Pero siempre la finalidad de una red es la de compartir información.

Consideraciones Generales

A continuación, junto con la referencia y definiciones ya mencionadas se mostrarán los roles y responsabilidades del ciclo de vida de la creación de la política de desarrollo seguro.

|  |  |
| --- | --- |
| **Roles** | **Responsabilidades** |
| **Encargado de seguridad de la información.** | Ejecutar labores de coordinación para una adecuada elaboración, revisión e implementación de esta política y las políticas y las materias que ella comprende. |
| **Comité de seguridad de la información.** | Hay que asegurar que las materias abordadas en esta política de ejecutan y se cumplen, identificar como se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la política detectando y proponiendo mejoras. |
| **Jefe departamento de Tecnologías de la información.** | Evaluar e implementar en caso de ser factible las propuestas de mejoras establecidas por el Comité de Seguridad de la información. Además de revisar periódicamente la política detectando y proponiendo mejoras. |
| **Personal / funcionarios Institución** | Cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política. Cada funcionario de la Institución deberá velar por la correcta implementación de las normas de desarrollo seguro de sistemas promovidos por la Institución dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de su equipo de trabajo. |
| **Personal externo** | Cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política. |

Desarrollo de Terceros

A continuación, en cuanto al desarrollo de sistemas por terceros, se deben crear contratos, con la empresa proveedoras, que contengan cláusulas, que resguarden la propiedad intelectual de la empresa, y, asimismo, aseguren los niveles de confidencialidad de la información, en el proyecto respectivo.

Se debe diferenciar, entre el encargado de celebrar y autorizar los contratos con terceros, de los que deben fiscalizar su cumplimiento

Desarrollo Interno

## Política de Desarrollo Seguro

La Política de Desarrollo Seguro comprende las reglas para el desarrollo de software y sistemas dentro de la organización. Para esto, se establecen los siguientes lineamientos:

* Se deberán utilizar técnicas de programación seguras tanto para los desarrollos nuevos como en las situaciones de reutilización de códigos donde es posible que no se conozcan las normas que se aplican al desarrollo o donde no sean coherentes con las buenas prácticas actuales. Lo anterior, tanto para el desarrollo interno como externo.
* Se deben estandarizar, los criterios de seguridad y calidad, que serán considerados, durante cada fase del proceso de desarrollo de sistemas de información.
* Se debe estandarizar el ciclo de vida del desarrollo de software logrando con ello los siguientes objetivos:   
  1. Definir actividades a llevarse a cabo en un proyecto de desarrollo de software.
  2. Unificar criterios en la organización para el desarrollo de software.

## Control de Acceso al Código Fuente de los Programas

Los sistemas creados necesitan de instancias de control que permitan monitorear el control de acceso al código fuente de los sistemas desarrollados con el propósito de establecer las responsabilidades sobre este y evitar cambios que puedan perjudicar a estos afectando su funcionalidad. El método para lograr esto se establece a continuación.

El miembro del personal que necesite de acceso a algún sistema debe realizarlo por medio del llenado de una Solicitud de Permisos y Accesos a Servidores, En ésta, el miembro del personal solicita acceso al código del sistema que necesita, tras lo cual, el Funcionario de Gestión Estratégica y Planificación (GEP) a cargo del proyecto debe firmar, otorgando el acceso al personal en caso de que así lo requieran, y el documento debe, posteriormente, ser entregado al Administrador de Redes, quién firma entregando acceso al usuario a los sistemas requeridos. Luego de esto el documento es devuelto al Funcionario de GEP dónde debe ser posteriormente almacenado.

Para la desvinculación del Funcionario de GEP a cargo del proyecto o sistema debe firmar el mismo documento.

**Nota:** El Administrador de Redes sólo puede firmar si el Funcionario de Desarrollo firmó ya que se entiende a este último como el primero que establece reconocimiento del caso y el primero que debe asumir la responsabilidad sobre un acceso no autorizado.

## Protección de Servicios de Aplicación en Redes Publicas

La información involucrada en los servicios de aplicación que pasan a través de redes públicas se deberá proteger contra la actividad fraudulenta, la disputa de contratos y la información y modificación no autorizada.

El software, datos y otra información que requiera un alto nivel de integridad y que estén accesibles públicamente se deben proteger por mecanismos adecuados. Los sistemas accesibles públicamente, se deben probar contra debilidades y fallas antes que la información esté disponible.

Debe haber un proceso de aprobación formal antes que la información esté accesible públicamente. Además, toda la entrada proveniente del exterior al sistema deberá ser verificada y aprobada.

Los sistemas electrónicos de edición, sobre todo aquellos que permiten la retroalimentación y el ingreso directo de información, se deben controlar con cuidado de modo que:

* La información se obtenga en cumplimiento con toda la legislación sobre protección de datos.
* El ingreso de la información a, y el procesamiento por, el sistema de edición será procesado completamente y con exactitud de manera oportuna.
* La información sensible será protegida durante la recolección, procesamiento y almacenamiento.
* El acceso al sistema de edición no debe permitir el acceso no planeado a redes las cuales se conecta el sistema.

## Entorno de Desarrollo Seguro

El entorno de desarrollo seguro en la institución considera los aspectos de seguridad de la información en:

* La fase de diseño de los proyectos de desarrollo de software y sistemas.
* El entorno de desarrollo, identificado como el conjunto de procesos y herramientas que se utilizan para desarrollar un código fuente o programa.
* El ciclo de desarrollo de software, en particular:
  + Seguridad en la metodología de desarrollo de software.
  + Pautas de codificación segura para cada lenguaje de programación que se utiliza.
* El establecimiento de puntos de verificación de seguridad dentro de los hitos de los proyectos de desarrollo de software y sistemas
* Los repositorios de información asociados a los proyectos de desarrollo de software y sistemas.
* El manejo del control de versiones de los proyectos de desarrollo de software y sistemas.
* La capacidad del equipo de desarrollo para:
  + Conocer las condiciones de seguridad de las aplicaciones desarrolladas.
  + Evitar, encontrar y resolver las vulnerabilidades de los desarrollos de software y sistemas.
* Los desarrollos ejecutados por personal externo y las condiciones contractuales con las empresas prestadoras de este servicio.

## Capacitaciones sobre Vulnerabilidades

El encargado de Seguridad de la Información, con apoyo del analista de seguridad de la información y/o el analista de ciberseguridad deben apoyar a sus miembros por medio de la educación a estos sobre las técnicas de codificación y código limpio con el propósito de evitar, encontrar y solucionar vulnerabilidades que puedan presentar sus sistemas acordes a las tecnologías que se aplican en el servicio y los lenguajes de comunicación que se apliquen.

Por otro lado, se debería tener en consideración una guía de codificación segura según el lenguaje que se utiliza que permita tener a disposición del personal de la unidad conocimiento sobre una forma de codificar segura y eficiente alrededor del lenguaje utilizado.

## PREVENCIÓN, REACCIÓN Y MITIGACIÓN DE VIOLACIONES DE SEGURIDAD

Esta sección presenta directrices para llevar a cabo procedimientos que garanticen una reacción adecuada a la ocurrencia de infracciones de seguridad. El uso de copias de seguridad, pruebas y manejo de eventos se detalla a continuación.

## Copias de seguridad

* La especificación de la necesidad y la asignación de la responsabilidad de hacer copias de seguridad de la base de datos y de los códigos fuente del sistema, así como las políticas de acceso para esta copia de seguridad, deben incluirse en el plan del proyecto.
* Se debe definir un procedimiento estructurado para restaurar las copias de seguridad.
* El personal a cargo de la recuperación de las copias de seguridad debe ser designado y capacitado adecuadamente.
* Se deben crear líneas de base de las versiones del sistema, lo que facilita la recuperación ágil a una versión anterior.
* La simulación de la restauración de datos debe llevarse a cabo de forma continua.

## Pruebas

* Las pruebas de seguridad manuales deben llevarse a cabo antes de cada versión del software que cambie su estructura (pantallas de inicio de sesión, servicios no autenticados, nuevos formularios con interacción del usuario, etc.).
* Se debe garantizar, a través de pruebas automatizadas, que los servicios y los datos confidenciales estén protegidos y estén disponibles solo para los usuarios que tengan la información.
* Se debe desarrollar una política de pruebas específica, ya sea automatizada o no, con el objetivo de garantizar la no vulnerabilidad a los principales ataques conocidos contra los sistemas.
* Los escenarios de prueba deben definirse para garantizar los requisitos de software no funcional, preferiblemente llevados a cabo por un equipo de prueba diferente del equipo de desarrollo de software, con el fin de evitar sesgos.
* Los escenarios de prueba deben definirse, principalmente en términos de seguridad, para los casos de actualizaciones de la arquitectura del sistema (servidores de aplicaciones, base de datos, versiones del navegador, versiones del sistema operativo, etc.).

## Separación de Entornos de Desarrollo, Prueba y Operacionales

Los ambientes de desarrollo, prueba y producción estarán separados preferentemente en forma física.

Para el caso de los desarrollos externalizados, se definirán y documentarán en los Términos de Referencia, detalladamente, las reglas y pasos para la transferencia de software, desde el estado de desarrollo hacia el estado productivo. Estas reglas deben considerar al menos los siguientes lineamientos:

* Ambiente de Desarrollo
* Ambiente de Pruebas
* Ambiente Pre-Producción
* Ambiente Producción

Al final del proyecto, se debe hacer traspaso de repositorio del proyecto.

En el caso de desarrollos internos se debe considerar:

* Ambiente de desarrollo
* Ambiente Pre-Producción
* Ambiente Producción

## Incidentes

* Se debe mantener un procedimiento planificado para la indisponibilidad inmediata del sistema y el mantenimiento correctivo.
* Se debe definir una política específica para fomentar el seguimiento de la respuesta a incidentes de violación de seguridad.
* Las lecciones aprendidas de incidentes pasados deben utilizarse para revisar la política de pruebas y aumentar la seguridad del sistema.

## Seguridad del Sistema

Todos los sistemas de información, durante su fase de desarrollo, se someterán a pruebas y verificaciones de seguridad, incluyendo un programa de actividades detallado, entradas de pruebas y los resultados esperados bajo una variedad de condiciones.

Se recomienda, que las pruebas del sistema incluyan, entre otros aspectos; instalación, volumen, rendimiento, almacenamiento, configuración, funcionalidad, seguridad, recuperación ante errores, como mínimo.

Dentro de lo posible, las pruebas, deben ser realizadas, almacenando criterios y datos de pruebas en archivos, de modo de permitir la verificación rápida y repetitiva.

Para manejar las vulnerabilidades se utilizó la herramienta ZAP de OWASP, este es un scanner de seguridad web de código abierto. Cuando se usa como servidor proxy permite a los usuarios manipular todo el tráfico que pasa a través de este, incluyendo el tráfico del protocolo seguro HTTPS.

## Pruebas de Aprobación del Sistema

Las pruebas de aceptación de sistemas se deberán realizar en un entorno de prueba (QA), de tal forma que permita, garantizar que el sistema no introducirá vulnerabilidades al entorno de la organización.

Asimismo, se debe asegurar, que las pruebas sean confiables.

Para realizar las pruebas de aceptación de sistemas, se podrán utilizar las herramientas automatizadas disponibles en el mercado, como las herramientas de análisis de códigos o los escáneres de vulnerabilidad y debería verificar la remediación de los defectos relacionados con la seguridad.

## Principios de Ingeniería Segura del Sistema

Se deben revisar de forma regular los sistemas con el propósito de asegurarse que estos se encuentren actualizados a las tecnologías y versiones existentes. Esto indica que se debe revisar de forma periódica los motores sobre los que trabajan los sistemas como apache, SQL, Linux, entre otros y la codificación para poder establecer que se mantenga segura en el tiempo.

Post Implementación y marcha blanca

El periodo de implementación y de marcha blanca darán a lugar dos meses luego de que el proyecto sea aceptado, el periodo de marcha blanca tendrá un tiempo de 2 periodos de revisión, es decir, 8 meses. Durante este tiempo todo el equipo TI estará listo para actuar en base a cualquier cambio o suceso que pueda ocurrir.

## Planifique su post implementación

Puede sonar elemental, pero planificar más allá de la salida a producción o go-live, es algo que no comprenden la mayoría de los ejecutivos y miembros del equipo del proyecto. Sobre todo, cuando están atrapados entre la maleza de una implementación. Sin embargo, ninguna organización alcanzará los beneficios empresariales esperados sin planificación ERP a largo plazo. Como resultado de la experiencia y de la investigación, las implementaciones de ERP exitosas hacen actividades de post implementación con una alta prioridad.

Periodo Revisión del Documento

La presente política entrará en vigor una vez aprobada y será transmitida por medio de correo institucional a todos los colaboradores.

También durante el periodo de marcha blanca se colocarán códigos QR en los distintos establecimientos de la institución, logrando entrar a una página con toda la información necesaria para comprender las nuevas políticas establecidas.

Se capacitarán a 2 personas del área más adecuada de cada establecimiento para poder lograr una mejor comprensión por parte de los colaboradores ayudando a diversificar el envío y entrega oportuno a todo el personal de la institución.

Periodo Revisión del Documento

Los periodos de revisión que serán utilizados para estas políticas de desarrollo sean trimestrales, proporcionando tiempo suficiente para poder suplir las necesidades del periodo anterior y prepararse para el siguiente.

Cabe recalcar que existen revisiones excepcionales para casos específicos de vulneración o incumplimiento de este.

Cada cambio debe ser aprobado por el secretario ejecutivo. Y el cumplimiento de este en una reunión con el comité de seguridad de forma trimestral, expresado anteriormente, con la finalidad de asegurar su cumplimiento e incorporación de todas las normas y procedimientos necesarios de implementar en el marco de la Ciberseguridad y Seguridad de la Información.