POLITICA DE DESARROLLO SEGURO DE LA DIRECCION DE SALUD DE LA CORPORACION MUNICIPAL DE VALPARAISO

AÑO 2022

	POLITICA DE DESARROLLO SEGURO DE LA DIRECCION DE SALUD DE LA CORPORACION MUNICIPAL DE VALPARAISO

FECHA: 21-09-2022		**VERSION:0.1**

	POLITICA DE DESARROLLO SEGURO DE LA DIRECCION DE SALUD DE LA CORPORACION MUNICIPAL DE VALPARAISO		
	FECHA: 21-09-2022		**VERSION:0.1**

Contenido

1. OBJETIVO GENERAL.

La presente política tiene como objetivo poder definir reglas y criterios transversales y controles de seguridad y confidencialidad para un Desarrollo Seguro, ya sea para desarrollo interno o desarrollo de terceros para la Dirección de Salud de la Corporación Municipal de Valparaíso.

2. ALCANCE.

La presente política de Desarrollo Seguro se aplica a todos los sistemas de información desarrollados y/o actualizados en la Dirección de Salud de la Corporación Municipal de Valparaíso, ya sea en forma interna como por empresas o profesionales externos contratados para tales efectos.

Esta política se aplica a todos los usuarios del DAS, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presten servicios en la dirección del DAS, a todos a quienes se les otorgue una casilla de correo electrónico institucional.

3. DOCUMENTOS DE REFERENCIA.

- Decreto Supremo N°83 del 03/06/2004 del Ministerio secretaría general de la Presidencia que "Aprueba Norma Técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos"
- Resolución Exenta N°1592, de 2017, de la Subsecretaria de salud Pública, que aprueba política Especial de seguridad para la adquisición, desarrollo y mantenimiento de sistemas de información para las Subsecretarias de Salud Pública y Redes Asistenciales.
- Resolución Exenta N°778, de 2014, del Ministerio de Salud, que Aprueba Política de Desarrollo de Sistemas.
- Decreto N°41, de 2012, del Ministerio de Salud, que aprueba reglamento sobre fichas clínicas:

- Regula el contenido, almacenamiento, administración, protección y eliminación de fichas clínicas de manera de resguardar el correcto empleo, disponibilidad y confidencialidad de estos.

4. DEFINICIONES.

Dirección de Salud (DAS)	Corresponde al Departamento de la Corporación Municipal de Valparaíso para la administración de la atención de la Salud Primaria en la comuna de Valparaíso.
Centro de Salud Familiar (CESFAM)	Corresponde a los cuidados básicos en salud, con acciones de promoción, prevención, curación, tratamiento, cuidados domiciliarios y rehabilitación de la salud; y atienden en forma ambulatoria.
Encargado de Seguridad de la información	Cargo definido como responsable de los procesos y procedimientos asociados a los protocolos y políticas que aseguren los recursos de la información del DAS.
Comité Técnico de Seguridad de la Información	Corresponde a la comisión encargada de la planificación y elaboración de políticas de seguridad de la información y sus mecanismos de control.
Unidad de Desarrollo y Soporte TIC	Equipo de trabajo cuyo enfoque es la generación, administración, mantención y soporte de aplicativos, programas, integraciones y soluciones utilizadas en los CESFAM como aquellas utilizadas en el DAS.
Proveedor	Personas naturales o jurídicas que tienen una relación contractual directa o indirecta con el DAS.
Riesgo	Probabilidad de ocurrencia de un evento indeseado con consecuencias negativas.

5. ROLES Y RESPONSABILIDADES.

Comité Único de Riesgo, de Calidad, y de Seguridad de la Información	❖ Velar por el cumplimiento y actualización de la Política General de Seguridad de la Información, presentando propuesta a la alta dirección para su aprobación. ❖ Validar, aprobar y difundir al interior del DAS Y CESFAM las políticas específicas de la Seguridad de la Información. ❖ Velar por la implementación de los controles de seguridad en el DAS y CESFAM. ❖ Gestionar la identificación, evaluación y mitigación de los riesgos que afectan los activos de información y la continuidad de negocio. ❖ Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados y proponer soluciones. ❖ Apoyar el desarrollo de los planes de comunicación, difusión y capacitación en materia de seguridad de la información. ❖ Conocer los incidentes que pudieran afectar a la seguridad de la información al interior de la organización, con el fin de establecer acciones preventivas y correctivas. ❖ Generar y proponer proyectos de desarrollo para el cumplimiento de los requisitos técnicos y normativos, dentro del marco presupuestario vigente. ❖ Informar a la alta dirección, en los intervalos que se convenga, sobre el Sistema de Seguridad de la Información
Encargado de Seguridad de la Información	❖ Velar por la implementación de las políticas de seguridad de la información al interior del DAS y CESFAM, de su control y de su correcta aplicación. ❖ Coordinar y gestionar la respuesta a incidentes que afecten a los activos de información de la Institución.
Dirección del Área de Salud	❖ Aprobar la Política General de Seguridad de la Información y de las estrategias y mecanismos de control para el tratamiento de los riesgos que afecten los activos de información de la Institución que se genere como resultado de los reportes o

	propuestas del Comité. Único de Riesgo, de Calidad y de Seguridad de la Información.
Unidad de Desarrollo y Soporte	❖ Cumplir con las disposiciones definidas en esta política ❖ Documentar el Sistema y/o sus modificaciones ❖ Recibir, canalizar y gestionar cualquier aviso de problema o incidente en la operación de los sistemas de información

6. DE LA POLÍTICA.

6.1 *Consideraciones Generales.*

La Unidad de Desarrollo y Soporte TIC, es la responsable de planificar y ejecutar el mantenimiento de los sistemas de la institución. Además, debe planificar y coordinar la ejecución de pruebas de funcionamiento de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.

Se debe estandarizar el ciclo de desarrollo de sistemas, tal como lo establece la metodología de desarrollo y mantención de sistemas definida en la Dirección de Salud de la Corporación Municipal de Valparaíso.

Se deben establecer estándares de criterios de seguridad y de calidad en el desarrollo de sistemas. Toda modificación de software crítico, por parches o módulos adicionales debe ser analizada previamente en los ambientes de desarrollo y prueba.

Se debe planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post-instalación, criterios de aceptación del cambio y un plan de vuelta atrás.

Los programadores y personal de terceros no deben tener acceso a información de producción que contenga datos sensibles.

Para propósitos de desarrollo y pruebas, las responsables deben generar sus propios datos, debiendo ser distintos a las que se encuentran en ambiente de producción.

Un sistema desarrollado o modificado por terceras partes debe cumplir con lo establecido en esta política, incluyendo los criterios de seguridad.

6.2 *Desarrollo por terceros.*

Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto.

Se debe diferenciar entre el encargado de establecer y autorizar los acuerdos con terceros, de las que deban auditar su cumplimiento.

6.3 *Gestión de Vulnerabilidades.*

Se debe establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software y proponer las medidas de mitigación al riesgo definido.

Se debe efectuar validaciones y evaluaciones periódicas de seguridad durante el ciclo de vida del proyecto. A lo menos una vez cada tres meses, se debe realizar un escaneo de las aplicaciones en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

6.4 *Documentación.*

El diccionario de datos debe mantener una descripción actualizada de las definiciones de datos.

Si el programador incluye comentarios en el programa fuente, estos deben ser útiles para un tercero y no divulgar información de configuración innecesaria.

Respecto a la documentación, esta se debe:

- Generar durante el ciclo de desarrollo y no postergar hasta el final.
- Revisar por los usuarios finales del sistema.
- Actualizar si el programa cambia alguna de sus funcionalidades
- Almacenar en un sitio centralizado (Servidor) administrado por la Unidad de Desarrollo y Soporte.

6.5 *Evaluación de casos de negocio.*

Como parte de las actividades a realizar en esta fase de un proyecto de desarrollo de un sistema de información, se debe clarificar la problemática actual referida a la seguridad de la información, que debe ser cubierta por el nuevo sistema.

En el estudio de factibilidad, se debe considerar el aspecto de seguridad, en cuanto al nivel de criticidad del sistema y de los controles que se debieran predefinir.

()

6.6 *Especificación detallada de requerimientos.*

En el análisis de factibilidad de los requerimientos, se debe considerar el nivel de criticidad del sistema, además del nivel de protección de seguridad que requieren los datos y las aplicaciones que lo componen.

Los requerimientos de seguridad deben ser compatibles con lo que se establece en las otras Políticas de Seguridad.

6.7 *Diseño del sistema.*

El nivel de sensibilidad debe ser definido para cada elemento de datos, archivo, programa y sistema. Si se define utilizar cifrado de datos, debe estar definido en el estándar de cifrados.

Si se utiliza un administrador de bases de datos, se debe emplear las herramientas de seguridad que el producto provee.

Todos los programas críticos deben incluir la generación de registros de auditoría, considerando como mínimo, la identidad del usuario que lee o escribe y la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.

En la etapa de diseño se debe proyectar el rendimiento esperado de un sistema informático, con el objetivo de no sobre dimensionar los recursos necesarios para el funcionamiento del Sistema (ancho de banda, RAM, recursos del servidor, etc.).

6.8 *Codificación y pruebas.*

No está permitido modificar programas sin que quede registrado o documentado el cambio. Se debe usar técnicas de programación modular, usando lenguajes de alto nivel.

No está permitido escribir o modificar código auto-copiante o cualquier otro tipo de código malicioso (virus y gusanos), así como funciones u operaciones no documentadas o no autorizadas en los programas.

En lo posible, las pruebas del sistema deberían incluir: instalación, rendimiento, almacenamiento, configuración, funcionalidad, seguridad, recuperación ante errores.

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

6.9 *Implementación.*

Se debe velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.

Se debe efectuar sintonía o ajuste (tuning) de los controles establecidos en la fase de diseño.

6.10 Post Implementación.

Se debe revisar y auditar la existencia de los controles de seguridad definidos en la etapa de diseño.

6.11Controles por implementar.

Se debe considerar e implementar, al menos, los siguientes controles:

1. Validación de datos de entrada y de salida.
2. Controles de procesamiento interno.
3. Controles criptográficos.
4. Protección de los datos de prueba.
5. Segregación de acceso a datos.

7. MECANISMOS DE DIFUSION Y DISTRIBUCION

Esta política, en su versión N°0.1 se encontrará vigente en página web de la dirección del Área de Salud de la Corporación Municipal de Valparaíso, en el footer, cuyo nombre será: Sistema de Seguridad de la información.

En encargado de seguridad de la información del DAS, velará por maximizar la cobertura de su difusión, a lo menos, a través de:

- Publicación de la página web de la dirección del DAS.
- Correo informativo.
- Entrega de los documentos directamente a cada funcionario del DAS y CESFAM.
- Capacitación a funcionarios o videos informativos de buenas prácticas

8. PERIODO DE REVISIÓN DEL DOCUMENTO

La revisión del contenido de esta política se efectuará, al menos, una vez al año, o atendiendo necesidades de cambios para garantizar su actualización, idoneidad, adecuación y efectividad en su ámbito de control

Sanción y excepciones