Política para la continuidad de la seguridad de información

Octubre 2024

Tabla de contenidos

1. Propósito

Esta política tiene como propósito de responder al nivel necesario de continuidad para la seguridad de la información durante situaciones adversas, a fin de evitar interrupciones en los activos críticos del negocio como consecuencia de fallas o desastres.

2. Alcance o ámbito de aplicación

Esta política aplica a todos los recursos computacionales del Hospital para los que es necesario controlar el acceso. Define el uso de nombres de usuario y contraseñas, así como sus solicitudes y administración.

Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el Hospital.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información (Nch-ISO 27001:2013)		
Nombre del Dominio	**ID Control ISO 27001**	**Nombre del Control**
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	A.17.1.1	Planificación de la continuidad de la seguridad de la información
	A.17.1.2	Implementación de la continuidad de la seguridad de la información
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información

3. Marco normativo

- NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
- El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
    - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
    - Leyes relacionadas
- Documentos relacionados:
    - Documento del Sistema de Gestión de Seguridad de la Información, disponibles en isalud.minsal.cl.

4. Roles y responsabilidades

- **Jefe de Unidad, Servicio o Centro de Responsabilidad**
    - Deberán nombrar al responsable administrativo con la debida experiencia para que elabore el Plan de Continuidad de Seguridad de la Información de los activos críticos que le competen, quien además debe deberá tener la disponibilidad de formar parte de los Comités y Equipos de Continuidad de Seguridad de la información, cuando se tomes acciones en esta materia.

- **Jefe Tecnologías de la Información y Comunicaciones**
    - Elaborar los Planes de Continuidad de Seguridad de la Información de los activos de Hardware y Software. Además de velar por una correcta ejecución de estos ante un evento que afecte la operación normal del Hospital.

- **Encargado de Seguridad de la Información**
    - Revisar y respaldar los planes formalizados en el Hospital y velar por la comunicación pertinente de estos al interior de la Institución.

5. Materias que aborda

- Planificación de la continuidad de la seguridad de la información.
- Implementación de la continuidad de la seguridad de la información.
- Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

6. Directrices de la política

6.1 Cumplimiento de la legislación

Las medidas de control de acceso a la información definidas deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales definidos en el documento “Normativa del Sistema de Gestión de Seguridad de la Información”.

6.2 Planificación de la continuidad de la seguridad de la información

El Hospital Carlos Van Buren establece que, dentro de su política los requisitos de seguridad de la información siguen siendo los mismos ante situaciones adversas (crisis o desastres), en comparación con las condiciones de operación normales.

Se deberán establecer, documentar, implementar y mantener los procesos, procedimientos y controles, para la continuidad de la seguridad de la información en caso de situaciones adversas, que reúna al menos los siguientes elementos:

- Análisis y determinación de los riesgos que se enfrentan en términos de probabilidad de ocurrencia de las amenazas e impacto, incluyendo la identificación y la determinación de la prioridad de los activos críticos para cada proceso.
- Identificación y evaluación de implementación de controles preventivos y de reducción de riesgo.
- Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información.
- Formulación y documentación de los planes de seguridad de la información.
- Prueba y actualización regular de los planes y procesos establecidos.

6.3 Implementación de la continuidad de la seguridad de la información

6.3.1 Responsabilidades.

Los responsables de los activos críticos del Hospital, deberán contar con una estructura de administración adecuada para prepararse, mitigar y responder ante un evento disruptivo que utiliza personal con la autoridad, la experiencia y la competencia necesaria.

Se deberá nominar al personal de respuesta ante incidentes con la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente y mantener la seguridad de la información.

Se deberá velar que se desarrollen y aprueben planes documentados, los procedimientos de respuesta y recuperación detallando cómo se administrará un evento disruptivo y mantendrá la seguridad de su información a un nivel predeterminado.

Tabla de responsables según los tipos de activos:

Activos	Tipo de activo	Responsable del plan de contingencia
HW Y SW	Software Base de datos Hardware Equipos informáticos Sistemas Formularios web	Dependencia TIC según corresponda
Otros	Documentos Expedientes	Jefe de la Unidad donde se desarrolla el proceso
	Personas	Jefe de la Unidad donde se desarrolla el proceso
	Infraestructura (edificios, equipamiento, etc.)	Jefe de la Unidad donde se desarrolla el proceso

6.3.2 Análisis previo para la generación de los planes de continuidad

Los responsables de cada tipo de activo de información deben realizar un análisis de los tipos de activos para determinar los requerimientos y prioridades de contingencia.

En el análisis se deben:

- Identificar los activos críticos del negocio.
- Identificar los eventos o cadenas de eventos que puedan ocasionar interrupciones en los procesos de negocio.
- Analizar y evaluar la probabilidad de ocurrencia y el impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información.
- Las evaluaciones deben considerar todos los activos de los negocios, no limitándose a los servicios de procesamiento de la información.
    - Se debe identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo: recursos críticos, impacto de las interrupciones, duración permitida de corte, prioridades de recuperación.

A partir de los resultados de este análisis, se deben desarrollar los planes de continuidad de seguridad de la información para los procesos y activos que sean clasificados como procesos críticos para la institución.

6.3.3 Desarrollo de los planes de continuidad.

Los responsables de los activos de información según corresponda, deberán elaborar los planes de continuidad de seguridad de la información previa a su implementación, así como crear y respaldar un plan para la implementación de estos.

En el proceso de planificación de la continuidad de la seguridad de la información se deben:

- Identificar todos los recursos y servicios relacionados al proceso de restauración, incluyendo personal, respaldos, acuerdos con terceras partes, y recursos no relacionados con el procesamiento de la información.
- Identificar prioridades y tiempos de recuperación para cada activo y/o procesos.
- Identificar, acordar y documentar todos los roles y responsabilidades, tanto internos como de empresas u organizaciones externas, para la ejecución del Plan.
- Identificar la pérdida aceptable de información y servicios.
- Establecer, documentar e implementar los procedimientos operativos a seguir, para permitir la recuperación y restauración de las operaciones del negocio y la disponibilidad de la información en las escalas de tiempo requeridas.

- Capacitar y/o difundir, de manera apropiada al personal, en los procedimientos y procesos acordados.
- Realizar revisiones, pruebas y actualización de los planes. Los resultados de las revisiones deben ser documentados.

Las copias de los planes de continuidad de la seguridad de la información y el material necesario para la ejecución de los mismos deben ser almacenadas en un lugar seguro a salvo de desastres del local principal y protegidas con el mismo nivel de seguridad que el local principal.

Los planes de seguridad de la información deben ser revisados y actualizados a lo menos cada 2 años.

6.3.4 Estructura de los planes de continuidad de la seguridad

Los aspectos que deben incluir los planes deben señalarse en el Plan respectivo, y debe incluir a lo menos:

- Las condiciones que se deben dar para la activación de cada plan.
- Los procedimientos de emergencia que describen las acciones a realizar tras un incidente que ponga en peligro las operaciones del negocio.
- Los procedimientos de respaldo que describen las acciones a realizar para desplazar las actividades esenciales del negocio, o servicios de soporte a lugares temporales alternos y para devolver la operatividad de los procesos de negocio en los tiempos requeridos.
- Los procedimientos operativos temporales a seguir mientras se termina la recuperación y restauración.
- Los procedimientos de restauración que describen las acciones a realizar para que las operaciones del negocio vuelvan a la normalidad.
- Un cronograma de mantenimiento que especifique cuándo y cómo se realizaran pruebas del plan y el proceso para el mantenimiento del mismo.
- Concientización, educación y formación del personal para comprender los procesos de continuidad de la información y garantizar que los mismos sean eficaces.
- Deben quedar establecidas las responsabilidades de las personas, en particular deberá quedar determinado quién es responsable de la ejecución de cada componente del plan, así como sus suplentes si fuera necesario y el plan de escalada.
- Los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y restauración.
- La efectiva gestión de las relaciones públicas, la eficiente coordinación con las autoridades apropiadas, como policía, bomberos, autoridades directivas, etc., y mecanismos eficaces

para convocar a quienes sean los responsables de los documentos electrónicos y sistemas informáticos afectados.

- Además de contar los contactos de apoyo ante dificultades técnicas u operacionales inesperadas de sistemas informáticos.

En el caso específico del jefe de Servicio, será quien aprueba los planes de seguridad de la información, sancionará las estrategias y asignará como los recursos necesarios para su ejecución.

6.4 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Los planes de continuidad se deben someter a pruebas, anuales para los activos de máxima criticidad y riesgo y de al menos dos años para el resto, y actualizar periódicamente.

Las pruebas deben asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son conscientes de los planes y sus responsabilidades, así como su actividad y rol a la hora de ejecutar el plan.

La programación de las pruebas para los planes de seguridad de la información debe indicar cómo y cuándo se va a probar cada elemento del plan.

Las pruebas deben incluir las siguientes técnicas para garantizar que los planes funcionaran en condiciones reales.

- Prueba sobre papel de varios escenarios (utilizando distintos ejemplos de interrupciones).
- Simulaciones (efectivas para la formación de personal).
- Pruebas de recuperación técnica (garantizando que los sistemas de información se puedan restaurar eficazmente.
- Pruebas de recuperación en lugar alterno.
- Pruebas de recursos y servicios de los proveedores externos (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído).
- Ensayos completos, en los que se verificará que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones.

Se debe asignar responsabilidades para las revisiones regulares de cada plan de continuidad.

El proceso formal de control de cambios deberá garantizar la distribución y el refuerzo de los planes actualizados.

Se debe tener especial atención con los cambios en:

- El equipamiento, incluyendo adquisición de equipos nuevos.
- Los sistemas.
- El personal.
- Las direcciones o números telefónicos.
- La estrategia del negocio.
- Los lugares, dispositivos o recursos.
- La legislación.
- Los proveedores y clientes principales.
- Los procesos existentes, nuevos o retirados.
- Los riesgos.

7. Mecanismo de difusión

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la intranet del HCVB http://10.6.96.210/menu/login.php
- Correo informativo.

8. Excepciones al cumplimiento de la política

Frente a casos de especiales, el Comité de Seguridad de la Información evaluará y podrá establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.