POLÍTICA DE CONTINUIDAD DE LAS OPERACIONES

DIRECCION DEL SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA

NOTA DE CONFIDENCIALIDAD

LA INFORMACIÓN CONTENIDA EN EL PRESENTE DOCUMENTO, ES DE PROPIEDAD Y USO EXCLUSIVO DEL SERVICIO DE SALUD VIÑA DEL MAR – QUILLOTA, PARA LOS FINES QUE DETERMINE, Y SOLO LOS FUNCIONARIOS DE ESTA INSTITUCIÓN EXPRESAMENTE AUTORIZADOS PODRÁN CONOCER Y UTILIZAR SU CONTENIDO DE ACUERDO A SU FINALIDAD.

Firmas de los responsables.

ELABORADO POR	REVISADO POR	APROBADO POR
Representante del Comité de Seguridad	Encargado de Seguridad	Director(a) del Servicio

SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA
DIRECCIÓN

INDICE

CONTROL DE VERSIONES

REVISIONES DEL DOCUMENTO DE POLITICA				
Nº Revisión	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
0(Cero)		Elaboración inicial	Todas	RCA
1				
2				
3				

1.- DECLARACIÓN INSTITUCIONAL

Se debe velar por el cumplimiento de la política de seguridad de la información establecida para todos los procesos normales y de excepción en la ejecución de las operaciones computacionales permitiendo así su continuidad de Servicio.

2.- OBJETIVOS DE LA POLÍTICA DE CONTINUIDAD EN LAS OPERACIONES

Esta política tiene como finalidad establecer los lineamientos generales y procedimientos para evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

3.- ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE CONTINUIDAD EN LAS OPERACIONES

Seguridad en las operaciones computacionales
- Continuidad del Negocio.
- Respuesta ante incidente.

4.- ROLES Y RESPONSABILIDADES

Director/a del Servicio de Salud de Viña del Mar- Quillota

- Sancionar las propuestas realizadas por el comité de seguridad, respecto a las políticas de continuidad en las operaciones
- Aprobar los recursos necesarios para implementación adecuada de las acciones comprometidas en la política de continuidad en las operaciones.

Comité de Seguridad

- Elaborar y aprobar la presente política de continuidad en las operaciones.
- Supervisar la implementación de la presente política.
- Proponer estrategias y soluciones específicas para la implementación de los controles necesarios para implantar la presente política.
- Monitorear los incidentes de seguridad y proponer estrategias para dar solución a las situaciones de riesgo detectadas en esta política.
- Monitorear el avance general en la implementación de la presente política.
- Divulgar la política de seguridad al interior de la institución.
- Implementar las medidas de seguridad definidas en la presente política.
- Mantener esta política de seguridad y sus procedimientos actualizados, con el fin de asegurar su vigencia y nivel de eficacia.

5.- MARCO GENERAL PARA LA POLÍTICA DE CONTINUIDAD EN LAS OPERACIONES

5.1.- MONITOREO Y DETECCIÓN DE ANORMALIDADES

- Todos los sistemas de producción críticos deben ser equipados con sistemas de detección de anormalidades que avisen al operador de turno cuando ocurra este tipo de eventos.
- Se debe establecer un conjunto formal de parámetros de sistemas a monitorear para cada tipo de plataforma, a fin de detectar situaciones anómalas. (definir los parámetros de seguridad que se monitorearan o que se exigirán a los proveedores).

5.2.- REVISIÓN DE REGISTROS DE AUDITORIA (LOGs)

- Todos los sistemas críticos deben configurarse para registrar los eventos de auditoria (logs) de las operaciones de administración y mantención, así como las condiciones de excepción.
- Los logs generados deben ser acumulados en forma segura en un sistema independiente y por un tiempo definido.
- Se deben programar revisiones periódicas de los logs en busca de condiciones anómalas y como verificación de los procedimientos establecidos de operaciones.

5.3.- PERSONAL DE RESPALDO

- Para los sistemas críticos debe existir la definición de personal de respaldo, para el caso que el encargado no esté disponible. En caso de algún impedimento para cumplir esta regla, es requisito contar con todos los procedimientos al detalle para la operación de dichos sistemas.

5.4.- DEFINICIÓN DE PROCEDIMIENTOS OPERACIONALES

- Establecer buenas prácticas de seguridad para las actividades más comunes que involucren sistemas menos críticos. (elaborar documento de buenas prácticas de seguridad)
- Todas las actividades de operación y mantención de los sistemas críticos deben estar expresamente definidas por procedimientos.
- Todo incidente debe ser debidamente notificado, documentado y revisado luego de su superación.
- Los procedimientos deben incluir, como mínimo:

  a) Procesamiento y manejo de la información.
  b) Programación de requerimientos previos o controles de secuencia de programas.
  c) Instrucciones para el manejo de condiciones de excepción.

d) Contactos de soporte adicional.
e) Instrucciones para el manejo de casos especiales.
f) Instrucciones de reinicio y recuperación en caso de falla del sistema.

5.5.- PROTECCIÓN DE PROCEDIMIENTOS OPERACIONALES

- Para los procedimientos y formularios de control de operación de los sistemas críticos, se debe velar por su mantención actualizada en el tiempo y se deben proteger del acceso de usuarios no autorizados.
- Identificar y clasificar la importancia de funciones esenciales para el servicio continuo. (secuencia de funciones esenciales para el servicio continuo).
- Definir límites de tiempo para la recuperación de cada elemento crítico de operaciones.(en base a secuencia definida en el punto anterior)
- Definir, documentar y probar medidas de prevención con cada elemento crítico.
- Definir, documentar y probar medidas de recuperación de catástrofe para cada elemento crítico de modo de entrenar al personal involucrado y para evaluar al procedimiento mismo.
- Mantener planes de continuidad operacional actualizados de acuerdo a los cambios que se producen en el tiempo. (sistema alternativo de emergencia que permita la continuidad operacional)

5.6.- CENTRALIZACIÓN DE LA INFORMACIÓN DE CONTACTOS

- Debe crearse una base de datos de contactos. (teléfonos, usuarios y contraseñas de sistemas, direcciones)
- Debe existir un rol de custodio de dicha información, quien será responsable de su mantención, garantizando su integridad, accesibilidad y actualización.

5.7.- DEFINICIÓN DE UN PLAN DE CONTINUIDAD OPERACIONAL DE SISTEMAS CRITICOS

- Se debe establecer cuáles son los procesos críticos, cuáles son los riesgos de tener esos procesos no-operativos y cuáles son los mecanismos de prevención y los procedimientos de recuperación.
- Establecer los planes de continuidad de operaciones de los sistemas definidos como críticos.
- Dentro de lo anterior, se debe definir los recursos necesarios, esto es: personal interno y externo, comunicaciones, hardware, software, infraestructura física y documentación.
- Dentro de la infraestructura física es importante determinar si se requerirá un site de respaldo y qué tipo de equipamiento debe tener.
- Debe existir un equipo de planificación de Continuidad Operacional que realice la tarea de análisis y programación. El equipo debe incluir representantes de variados sectores de la organización que permitan un manejo consensuado y ejecutivo del

problema. Quien lidere este grupo, debe reportar directamente al Comité de Seguridad de la Información.

5.8.- SEPARACIÓN DE ÁREAS Y FUNCIONES

- Las instalaciones, funciones y personal del Subdepartamento de TI debe mantenerse en forma independiente y en áreas separadas.
- La responsabilidad de ejecución y control de procesos críticos no debería recaer en una sola persona, atendiendo al principio de segregación de funciones.

6.- APLICACIÓN PARA LA POLÍTICA DE CONTINUIDAD EN LAS OPERACIONES

La infracción a las obligaciones establecidas en esta norma, podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley Nº 18.834, sobre Estatuto Administrativo. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

El Subdepartamento de TI no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de continuidad en las operaciones.

7.- MONITOREO

El Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota verificará la aplicación de estas políticas en la continuidad de las operaciones.

8.- GLOSARIO DE TERMINOS

- RRFF: Recursos Físicos
- RRHH: Recursos Humanos
- TI: Tecnologías de Información
- LOGs: Registro de eventos durante un rango de tiempo en particular
- Site: Central de Servidores y/o Comunicaciones