MINISTERIO DE SALUD

SIS Seguro Integral de Salud

Nº 159 -2013/SIS

RESOLUCIÓN JEFATURAL

Lima, 09 AGO 2013

VISTO: El Informe Nº 008-2013-SIS-OGTI-JCZ; el Proveído Nº 190-2013-SIS/OGTI de la Oficina General de Tecnología de la Información; y el Proveído Nº 449-2013-SIS/OGAJ de la Oficina General de Asesoría Jurídica;

CONSIDERANDO:

Que, por Ley Nº 27657, Ley del Ministerio de Salud, se crea el Seguro Integral de Salud, como Organismo Público Descentralizado del Ministerio de Salud, siendo calificado por Ley N° 29158, Ley Orgánica del Poder Ejecutivo, y Decreto Supremo N° 034-2008-PCM, como Organismo Público Ejecutor;

Que, mediante Resolución Ministerial Nº 129-2012-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática;

Que, mediante Resolución Jefatural Nº 114-2013/SIS se designa a la coordinadora que hará las veces de Oficial de Seguridad de la Información, y responsable de la implementación de las disposiciones establecidas en la Resolución Ministerial Nº 129-2012-PCM; asimismo con Resolución Jefatural Nº 116-2013/SIS se constituye el "Comité de Gestión de Seguridad de la Información" de carácter permanente en el Seguro Integral de Salud;

Que, mediante documentos de vistos se sustenta la necesidad de aprobar la Política de Seguridad de la Información del Seguro Integral de Salud, de acuerdo a los parámetros establecidos en la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos";

Con el visto bueno de la Secretaría General, de la Oficina General de Tecnología de la Información, y con la opinión favorable de la Oficina General de Asesoría Jurídica;

De conformidad con lo establecido en el numeral 11.8 del artículo 11º del Reglamento de Organización y Funciones del Seguro Integral de Salud, aprobado por Decreto Supremo Nº 011-2011-SA

SE RESUELVE:

Artículo 1º.- Aprobar la "Política de Seguridad de la Información del Seguro Integral de Salud", la misma que forma parte integrante de la presente Resolución.

Artículo 2º.- Encargar a la Secretaría General en coordinación con la Oficina General de Tecnología de la Información, publique la presente Resolución en el Portal Institucional del Seguro Integral de Salud.

Registrese y comuníquese,

PEDRO FIDEL GRILLO ROJAS
Jefe del Seguro Integral de Salud

POLITICA DE SEGURIDAD DE LA INFORMACIÓN DEL SEGURO INTEGRAL DE SALUD (SIS)

Versión 1.0

Julio 2013

INDICE

1. INTRODUCCION 5
2. OBJETIVOS 5
3. ALCANCE DE LAS POLÍTICAS 5
4. BASE LEGAL 5
5. REVISIÓN Y ACTUALIZACIÓN 6
6. DEFINICIONES 6
7. POLÍTICA 10
7.1 Seguridad Organizacional 10
7.2 Gestión de Activos 12
7.3 Seguridad en Recursos Humanos 12
7.4 Seguridad física y del entorno 13
7.5 Gestión de comunicaciones y operaciones 14
7.6 Control de acceso 15
7.7 Adquisición, desarrollo y mantenimiento de sistemas de información 15
7.8 Gestión de incidentes en la Seguridad de la Información 16
7.9 Gestión de la Continuidad del negocio 16
7.10 Cumplimiento 17

Control de Versiones

Versión	Fecha Elaboración	Fecha Vigencia	Descripción	Código
1.0	04/07/2013	DESDE 17/07/2013	Elaboración de la Política de Seguridad de la Información	OGTI-SI-SGSI-POLT-001

AUTORIZACIONES Y RESPONSABLES

Responsables de la aprobación, revisión y elaboración del presente documento:

APROBÓ:

FECHA	PUESTO	NOMBRE	FIRMA
17/07/2013	JEFE DEL SEGURO INTEGRAL DE SALUD.	PEDRO FIDEL GRILLO ROJAS	

REVISÓ:

FECHA	CARGO	NOMBRE	FIRMA
17/07/2013	JEFE DEL SEGURO INTEGRAL DE SALUD.	PEDRO FIDEL GRILLO ROJAS	
	JEFE ADJUNTO	JULIO SEGUNDO ACOSTA POLO	
	SECRETARÍA GENERAL	PATRICIA PAMELA PASTOR MANSILLA	
	DIRECTOR GENERAL DE LA OFICINA GENERAL DE ADMINISTRACIÓN DE RECURSOS.	LUIS FELIPE COCA SILVA	
	DIRECTOR GENERAL DE LA OFICINA GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN.	VICTOR GERMAN CHAVEZ BAHAMONDE	
	DIRECTORA GENERAL DE LA OFICINA GENERAL DE PLANEAMIENTO, PRESUPUESTO Y DESARROLLO ORGANIZACIONAL.	SARA LUZ HURTADO CRISTOBAL	
	DIRECTOR GENERAL DE LA OFICINA GENERAL DE ASESORÍA JURÍDICA.	IVAN ALFREDO ZANETTI PEINADO	
	DIRECTORA GENERAL DE LA OFICINA GENERAL DE IMAGEN INSTITUCIONAL Y TRANSPARENCIA.	MARTA VERONICA YNES ALIAGA HERRERA	
	GERENTE DE LA GERENCIA DEL ASEGURADO	TERESA LEONOR SALAZAR ALLAIN	
	GERENTE DE LA GERENCIA DE RIESGO Y EVALUACIÓN DE LAS PRESTACIONES	NILDA TERRONES VALERA	
	GERENTE DE LA GERENCIA DE NEGOCIOS Y FINANCIAMIENTO.	ALAN PAUL VALDIVIA MIRANDA	

ELABORÓ:

FECHA	CARGO	NOMBRE	FIRMA
04/07/2013	COORDINADORA DE SEGURIDAD DE LA INFORMACIÓN	JENNY CASTAÑEDA ZUBIAUR	

1. INTRODUCCION

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Eso es muy importante en el creciente ambiente interconectado de negocios donde la información esta expuesta a un mayor rango de amenazas y vulnerabilidades.

Se considera que la información puede encontrarse en medio impreso, escrito, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación.

La seguridad de la información protege a esta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizando los daños a la organización.

2. OBJETIVOS

Proteger los recursos de información del SIS y la tecnología utilizada para su procesamiento frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Analizar y planificar la reducción del riesgo de pérdida, robo o revelación de información.

3. ALCANCE DE LAS POLÍTICAS

Esta política y los documentos que se generen de esta, deben ser cumplidas por todo personal que labore en el Seguro integral de Salud (SIS) bajo cualquier modalidad de contrato. Además de proveedores de servicios e Instituciones con las que el SIS firme Convenios de Colaboración Interinstitucional y su personal.

4. BASE LEGAL

- Resolución Ministerial Nº 129-2012-PCM
- Resolución Ministerial Nº 246-2007-PCM.
- Norma Técnica Peruana "NTP-ISO EC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información. Requisitos"
- Norma Técnica "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. 2ª Edición"

5. REVISIÓN Y ACTUALIZACIÓN

Se debe mantener la Política de Seguridad del SIS actualizada, a efectos de asegurar su vigencia y nivel de eficacia, por lo cual será revisada anualmente y/o cuando ocurran cambios significativos con la finalidad de asegurar la adecuación y efectividad continua.

Los documentos que se generen como consecuencia del desarrollo de la presente política, debe ser actualizado dinámicamente en la medida que los procesos y la infraestructura informática del SIS cambie.

6. DEFINICIONES

- **Acción correctiva**: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.
- **Acción preventiva:** Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.
- **Aceptación del Riesgo:** Según [ISO/IEC Guía 73:2002]: Decisión de aceptar un riesgo.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.
- **Alcance:** Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.
- **Alerta:** Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.
- **Ambiente:** Se refiere al ambiente de trabajo apropiado según el caso que se defina.
- **Amenaza:** Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Análisis de riesgos:** Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Análisis de riesgos cualitativo:** Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.
- **Análisis de riesgos cuantitativo:** Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **CID:** Acrónimo español de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.
- **Checklist:** Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia

del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.
- **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]: característica/propiedad por la que la información no está disponible o es revelada a individuos, entidades, o procesos no autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.
- **Control detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- **Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza, por ejemplo, por medio de avisos disuasorios.
- **Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
- **Directiva:** Descripción que clarifica qué deberia ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Disponibilidad:** Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
- **Evaluación de riesgos:** Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Evento:** Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o

test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Impacto:** El costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros –por ejemplo, pérdida de reputación, implicaciones legales, entre otros.
- **Incidente:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Infraestructura Tecnológica:** Se encuentra integrada por un conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, entre otros), software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración, entre otros) y servicios (soporte técnico, seguros, comunicaciones, entre otros); que en conjunto dan soporte a las aplicaciones (sistemas informáticos) de una empresa.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, entre los principales) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.
- **ISO 27002:** Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.
- **No conformidad: (NC)** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

- **PDCA (Plan-Do-Check-Act):** Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).
- **Plan de continuidad del negocio (PCN)**: Orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos:** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.
- **Política de escritorio limpio:** La política de la empresa que indica a los empleados que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.
- **Propietario:** Identifica a la persona que tiene responsabilidad aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.
- **Riesgo Residual:** Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.
- **Segregación de tareas:** Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- **Seguridad de la información:** Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.
- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).
- **Servicios de tratamiento de información:** Según [ISO/IEC 27002:2005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

S. HURTADO C. I. Zanetti J.ACOSTA P. Grillo

- **TI:** Tecnología de la Información.
- **Tratamiento de riesgos:** Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.
- **Valoración de riesgos:** Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.
- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. (Fuente: Glosario de Términos ISO 27000).

M.ALIAGA

7. POLÍTICA

La Política General de la Gestión de la Seguridad de la Información, que permita mitigar el riesgo informático del Seguro integral de Salud (SIS), esta basada en el mantenimiento de los registros adecuados que permita garantizar el cumplimiento de las normas, controles, estándares, procedimientos y otros que se definan en el ámbito informático de la Institución.

A. VALDIVIA

L.F. Coca S.

La presente política, los procedimientos y los estándares que tengan asociados, deben ser cumplidos por todo personal que labore en el Seguro integral de Salud (SIS) bajo cualquier modalidad de contrato. Además de proveedores de servicios e Instituciones con las que el SIS firme Convenios de Colaboración Interinstitucional y su personal.

7.1 Seguridad Organizacional

Con la finalidad de administrar la seguridad de la información dentro del SIS, se mantendrá una estructura interna de seguridad de la información que permita definir e implementar los controles necesarios para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

G. Chávez B.

a) Oficial de Seguridad de la Información, designado por Resolución Jefatural Nº 114-2013/SIS, cuyas funciones son:

- ✓ Definir y actualizar políticas, normas, procedimientos y estándares del SGSI.
- ✓ Realizar el análisis de riesgo a las aplicaciones.
- ✓ Asesorar en la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio.
- ✓ Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información.
- ✓ Dar los lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios.

T.Salazar A

S. HURTADO C.

I. Zanetti

J.ACOSTA

P. Grillo

- ✓ Promover la formación, educación y el entrenamiento en seguridad de la información.
- ✓ Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes.
- ✓ Realizar estudios de penetración y pruebas de seguridad en todos los ambientes (Desarrollo, Pruebas, Producción y Contingencia).

b) Comité de Gestión de Seguridad de la Información, designado por Resolución Jefatural Nº 116-2013/SIS, cuyas funciones son:

- ✓ Es el primer nivel de aprobación, revisión, rechazo, modificación o eliminación de las Políticas de Seguridad de la Información, normas y procedimientos.
- ✓ Debe revisar periódicamente el estado general de la seguridad de la información.
- ✓ Revisar y monitorear los incidentes de seguridad de la información.
- ✓ Establecer recursos para administrar los incidentes de seguridad u otras vulnerabilidades.
- ✓ Revisar y aprobar los proyectos de seguridad de la información.
- ✓ Realizar otras actividades de alto nivel relacionadas con la seguridad de la información

c) Seguridad con Terceros

- ✓ Todas las conexiones de terceros hacia la red interna del SIS deben ser autorizadas, revisadas y monitoreadas por la Oficina General de Tecnología de la Información (OGTI).
- ✓ Los contratos de desarrollo o mantenimiento de Software que se suscriban con terceros, deberán incluir el acuerdo para cumplir las políticas de seguridad de la Información establecidas por el SIS.
- ✓ Además, los contratos para los cuales se transfiere la responsabilidad por la seguridad de la información a un tercero (outsourcing), deben dejar en forma explícita el compromiso por parte de este, de la aplicación de los Controles de seguridad necesarios en la medida en que el SIS le haya transferido dicha responsabilidad.

d) Acuerdos de Seguridad

- ✓ Todo personal que labore en el SIS bajo cualquier modalidad de contrato y terceros que deban realizar labores dentro de la institución, sea por medios lógicos o físicos que involucren el manejo de información del SIS, deben conocer, entender,

firmar y aceptar la correspondiente acuerdo de confidencialidad de la información que para su caso aplique.

- ✓ Todos están obligados a continuar protegiendo la información del SIS cumpliendo las políticas de seguridad después de terminar su relación con la entidad.

e) Responsabilidad por la información

- ✓ Cada conjunto de datos tendrá un usuario dueño y responsable de los datos que están en producción. Donde se entiende por dueño de la información al usuario que trabaja con la información y como responsable de la información al Director del área donde ésta se genera.
- ✓ Es responsabilidad de la Oficina General de Tecnología de Información, mantener segura la información sistematizada del SIS.

f) Segregación de Funciones

- ✓ El SIS debe asegurar que los procesos se desarrollen a través de una correcta segregación de funciones que permita garantizar la ejecución, la revisión, la autorización y el seguimiento se dan a diferentes niveles.

7.2 Gestión de Activos

- El SIS realizará y mantendrá un inventario de sus activos de información, identificando a sus propietarios.
- Un responsable de cada oficina mantendrá actualizado el inventario de activos de información que poseen.
- Se debe realizar un control sobre todo software y hardware que sea recibido, adquirido o arrendado, hasta su retiro de uso.
- El SIS realizará una clasificación de la información en base a las tres características de la seguridad de la información: confidencialidad, integridad y disponibilidad. Teniendo como resultado tres categorías:
  - ✓ CRITICIDAD BAJA
  - ✓ CRITICIDAD MEDIA
  - ✓ CRITICIDAD ALTA

7.3 Seguridad en Recursos Humanos

- El SIS, a través del área de Recursos Humanos, realizará la verificación de antecedentes, de conformidad con la legislación laboral vigente.
- Durante el proceso de selección de personal, las funciones y las responsabilidades de seguridad de la información deben ser comunicadas claramente a los candidatos. De igual manera es

responsabilidad de todo personal vinculado al SIS con anterioridad a la elaboración de este documento, conocer, entender y asumir sus responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar.

- El incumplimiento de esta Política de Seguridad de la Información así como de las normas, procedimientos y formatos que regulan el SGSI que conlleve a un incidente de seguridad, implicará un proceso disciplinario y/o las acciones legales correspondientes, dentro del marco legal vigente, por parte del SIS para establecer la responsabilidad del usuario involucrado.
- Se contará con procedimientos ante la finalización del contrato, que implique devolución previa de activos de información como software, documentación, equipos, dispositivos móviles, llaves, fotocheck e información que resida en medio almacenamiento electrónico.
- El SIS, a través del área de RRHH y el Oficial de Seguridad de la Información, planificara labores de concientización y entrenamiento a todo el personal en temas de Seguridad de la información.

7.4 Seguridad física y del entorno

- A fin de evitar el acceso no autorizado todos los trabajadores deberán ingresar a la institución portando el fotocheck que se les ha asignado.
- Todo acceso de proveedores de servicios o terceros debe ser autorizado y monitoreado, así también, deberán contar con un fotocheck temporal asignado al momento de su ingreso.
- Todo dispositivo y equipamiento que almacene y/o procese información restringida o confidencial, deben ser protegidos de acceso no autorizado y ubicados en un lugar seguro o en un ambiente diseñado para el resguardo de dicha información.
- Todas las instalaciones contarán con equipo apropiado contra incendios que debe ser provisto y ubicado adecuadamente.
- El acceso al Centro de Datos y áreas de trabajo que manejen información restringida o confidencial, será supervisado registrando el ingreso y salida.
- Todos los servicios públicos de soporte como electricidad, agua, desagüe y aire acondicionado deben ser adecuados para los servicios de tratamiento de información que soportan.
- Se deberá contar con un plan de mantenimiento de equipos, que minimice problemas de disponibilidad de servicio.

- Todo equipo portátil de propiedad del SIS, que contenga información restringida y/o confidencialidad y que pueda ser transportada fuera de las instalaciones del SIS, deberá contemplar mecanismos de encriptación de los datos.

7.5 Gestión de comunicaciones y operaciones

- Los procesos operativos donde se trate información deben contar con documentación y puestos a disposición de quien le competa.
- Se debe llevar un control de cambios sobre la plataforma tecnológica y aplicaciones en producción así también como la documentación de esta.
- Los recursos informáticos del SIS deben ser utilizados únicamente con propósitos de la institución.
- El SIS podrá proporcionar acceso remoto a sus contratados previa evaluación y autorización. La OGTI garantizará un esquema de seguridad para los mismos.
- La instalación de antivirus es obligatoria y será considerada como parte de la instalación inicial. Estos programas serán actualizados periódicamente, mediante mecanismos automáticos o manuales.
- Se contará con un servicio de respaldo para asegurar que toda la información crítica o confidencial este disponible tras un desastre o una falla.
- Los backups y la documentación relacionada serán resguardados en un lugar seguro diferente al Centro de Cómputo.
- Se contará con un plan de validación de los procedimientos de recuperación para asegurar que son eficaces.
- Se gestionará el uso de dispositivos de almacenamiento masivo (grabadores de CD, USB ó similares) en las estaciones de trabajo, en caso sea necesario se bloqueará el uso de dichos dispositivos, o se gestionará el permiso con el Oficial de Seguridad de la Información a fin establecer los mecanismos de seguridad apropiados.
- Se considerará los procedimientos necesarios para eliminar los medios informáticos de forma segura y sin peligro.
- Se considerará los procedimientos necesarios para el intercambio de información con terceros.
- Se monitoreará y registrará todas las actividades relacionadas a eventos de seguridad sin exceptuar a los administradores y operadores. Este proceso debe ser sistematizado.
- Los relojes de los sistemas que procesan información estarán sincronizados.

7.6 Control de acceso

- Se establecerá procedimientos para el control de acceso a los sistemas de información, previniendo accesos o modificaciones no autorizados. Así también política de contraseña que regule el uso de estas.
- El acceso a los servicios de tratamiento de información ser realizaran previa asignación un identificador único y una contraseña y de acuerdo a las funciones que desempeña.
- Los Propietarios de Información o responsables de la Información son los responsables de definir y gestionar el acceso que debe tener el personal a su cargo los cuales serán verificados según un plan de revisión.
- Solo se permitirá el uso de identificadores genéricos por razones comerciales u operacionales, los que previamente deberán ser aprobados, documentados e informados al Oficial de Seguridad de la Información.
- Los usuarios de los sistemas de tratamiento de información deberán mantener la confidencialidad de las contraseñas.
- Se deberá mantener políticas de pantalla e escritorio limpio.
- El acceso a los servicios de red, tanto internos como externos debe ser controlado, de manera que los usuarios no comprometan la seguridad de los activos de información.
- Las sesiones de los sistemas que excedan el tiempo máximo de inactividad deben ser automáticamente finalizadas.
- Se debe establecer procedimientos de seguridad de la información para el acceso remoto a los recursos informáticos.
- Todo acceso remoto a los terminales o equipos deberá ser realizado solo mediante el uso de herramientas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

7.7 Adquisición, desarrollo y mantenimiento de sistemas de información

- Los requerimientos del negocio para sistemas nuevos o mejoras a los sistemas existentes deben cumplir con controles en materia de Seguridad de la Información.
- La participación del Oficial de Seguridad de la Información en los proyectos de desarrollo o adquisición de sistemas debe ser desde la Fase de Requerimientos y en las demás fases del Ciclo de Vida de Desarrollo de Software, en coordinación con el responsable del proyecto.

- El SIS mediante la OGTI deberá contar con metodologías estandarizadas para la adquisición, desarrollo y mantenimiento de los sistemas de información.
- Como parte del Desarrollo de Software se debe validar los datos de entrada y salida de las aplicaciones para garantizar que son correctas y apropiadas.
- Se deberá documentar y hacer cumplir los procedimientos formales de control de cambios.
- Se debe mantener la separación de ambientes de prueba de los ambientes de producción que permitan segregar funciones y verificar los sistemas antes de su pase a producción.
- El acceso al código fuente, diseños, requerimientos, planes de pruebas y documentación relacionada a los sistemas de información, se deberán controlar a fin de evitar la introducción de cambios no autorizados, para lo cual se mantendrá el registro del usuario, fecha y motivo del acceso o cambio registrado.
- El desarrollo de software por terceros deberá ser supervisado y monitoreado por la OGTI.
- Se deberá definir y establecer los roles y responsabilidades asociadas con la gestión de las vulnerabilidades técnicas.

7.8 Gestión de incidentes en la Seguridad de la Información

- Los trabajadores del SIS deben de reportar los incidentes de seguridad de la información que detecten al Oficial de Seguridad de la información lo antes posible.
- Las fallas que se detecten en las aplicaciones del SIS también serán consideradas como incidentes de seguridad de la información porque afectan la disponibilidad de la información.
- El Oficial de Seguridad establecerá el procedimiento para el reporte y seguimiento del incidente de seguridad de la información.
- Periódicamente se analizará los reportes de incidentes de seguridad de la información a fin de plantear mejoras ante futuros incidentes, previniendo la recurrencia de los mismos.

7.9 Gestión de la Continuidad del negocio

El Comité de Seguridad de la Información propondrá un plan de continuidad de negocio (BCP) considerando los requerimientos de Seguridad de la Información del SIS, este plan debe ser cumplido por todo el personal de la Institución.

Se realizará pruebas periódicas y mantenimiento del Plan de Continuidad de Negocio del SIS con una frecuencia mínima anual.

M.ALIAGA

A. VALDIVIA

L.F. Coca S.

I. Chávez B.

T.Salazar A.

S. HURTADO C.

I. Zanetti

J.ACOSTA

P. Grillo

7.10 Cumplimiento

- Todas las legislaciones, regulaciones y requerimientos contractuales que sean importantes para los sistemas de información y el SIS deben ser identificados, documentados y actualizados.
- El SIS deberá mantener los documentos que acrediten la propiedad de las licencias, material original, manuales, entre otros.
- Los trabajadores, proveedores de servicios y terceros deben ser disuadidos de utilizar los servicios de tratamiento de información del SIS para propósitos no autorizados.
- El Oficial de Seguridad de la Información deberá evaluar el cumplimiento de las Políticas de Seguridad de la Información implantadas.
- Se planificará auditorias de los servicios de tratamiento de información del SIS usando herramientas especializadas para evitar su mal uso.