# POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL SGSI DE AREVALO S.A

**Control Documental**

| Versión | Autor | Fecha | Descripción |
|---|---|---|---|
| 1.0 | UOC-MISTIC | Marzo 28 2013 | Versión Inicial |

**Revisión del Documento**

| Nombre | Cargo | Versión | Fecha | Comentarios |
|---|---|---|---|---|
| Gustavo Arévalo Arenas | Gerente de Proyecto | 1.0 | Marzo 28 2013 | Ninguno |

**Aprobación del Documento**

| Versión | Aprobación | Fecha | Descripción |
|---|---|---|---|
| Gustavo Arévalo Arenas | Gerente de Proyecto | Marzo 28 2013 | Ninguno |

# CONTENIDO

# 1 INTRODUCCIÓN

La información relacionada con los procesos de negocio de AREVALO S.A, es un activo de mucho valor para la organización, por lo tanto requiere una protección del uso no adecuado, de su publicación no autorizada, de robo, alteración o destrucción. Una gestión de seguridad de la información efectiva garantiza que pueda ser compartida mientras se minimiza su exposición al riesgo.

Amenazas que pueden afectar la seguridad de la información se incluyen, pero no se limitan a:

- Error.
- Fraude.
- Código malicioso.
- Desastres naturales.
- Terrorismo.
- Espionaje.
- Interrupción del Servicio.
- Hackers.
- Sabotaje

Esta Política de Seguridad de la Información del SGSI se ha desarrollado para garantizar la confidencialidad, integridad y disponibilidad de la información y de los activos (ej.: sistemas de información, aplicaciones, instalaciones, etc.) de los procesos de negocio de AREVALO S.A, y está alineada con el estándar de industria ISO 27001 “Requerimientos – Sistema de Gestión de Seguridad de la Información – Técnicas de seguridad – Tecnologías de Información”. Al implementar esta política todas las personas involucradas, tanto empleados como proveedores, deben garantizar la protección de los procesos, la reputación y la mejora continua.

# 2 Alcance

La política de Seguridad de la Información del SGSI aplica a todos los activos de información, equipos de proveedores y terceros que crean, procesan o resguardan la información de los procesos de negocio de AREVALO S.A.

Está dirigida a funcionarios, proveedores, contratistas, consultores y demás terceros que utilicen información dentro de los procesos de negocio.

La garantía del cumplimiento de está política debe ser responsabilidad de todos y cada uno de los que intervienen en los procesos y su cumplimiento será auditado por los entes de control interno de la AREVALO S.A.

# 3 Audiencia

La presente política debe ser publicada con el fin de que sea conocida, aceptada y cumplida por los empleados, proveedores y clientes que crean, procesan o resguardan la información de AREVALO S.A. Esta política aplica a:

- Todos los empleados que soportan las actividades de gestión y soporte de los procesos de negocio.
- Todos los proveedores y socios estratégicos que aportan en la gestión de operaciones de los procesos de negocio.
- La relación con compañías u organizaciones externas que comparten información con AREVALO S.A.
- Toda la tecnología y actividades de procesamiento de información de los procesos de negocio.

# 4 Sistema de Gestión de Seguridad de la Información

Un sistema de gestión de seguridad de la información (SGSI), es un marco que define la metodología con la cual AREVALO S.A protege los activos de sus procesos de negocio y garantiza que las medidas de seguridad apropiadas son implementadas. Es responsabilidad del Proceso de Seguridad de la Información la creación y documentación de un SGSI y de los controles asociados.

El SGSI debe ser desarrollado adoptando el modelo PHVA (Planear, Hacer, Verificar y Actuar). Los componentes básicos de dicho modelo se resumen a continuación:

| | |
|---|---|
| Planear | Establecer el SGSI con la creación de políticas, estándares, procedimientos, estructura organizacional y procesos de seguridad relacionados con infraestructura tecnológica y no tecnológica; con el fin de identificar, analizar y tratar el riesgo, para garantizar el cumplimiento de la seguridad y los objetivos de negocio de AREVALO S.A. |
| Hacer | Implementar, operar y monitorear las políticas creadas para el SGSI. |
| Verificar | Revisar la efectividad del SGSI. |
| Actuar | Mantener y mejorar el SGSI basado en los resultados de la fase de Verificación. |

## 4.1 Planear: Planear el SGSI

Los requerimientos de objetivos de control y controles definidos en esta política deben ser implementados como la base para el desarrollo del SGSI. Este SGSI debe establecerse para cumplir con los requerimientos y para gestionar el riesgo a niveles aceptables. Los controles definidos en el presente documento deben ser implementados por todos y cada uno de los empleados, proveedores y usuarios si sus actividades o labores lo requieren.

La gestión de los riesgos identificados se debe llevar a cabo utilizando el proceso definido a continuación.

1. La política del SGSI debe incluir, pero no estar limitada a lo siguiente:

    - Un marco de trabajo documentado para definir el alcance, los límites y objetivos para establecer una dirección y principios de acción soportados en la seguridad de la información.
    - Análisis y documentación de los requerimientos de negocio, legales y regulatorios, y obligaciones de seguridad contractuales específicas de los procesos de negocio.
    - Una metodología de análisis de riesgo donde se establezcan los criterios de que riesgos serán evaluados y como se identificarán los niveles de riesgos.

2. Un responsable del proceso debe llevar a cabo el análisis de riesgo del proceso y debe mantenerlo y gestionarlo para toda la información y la infraestructura tecnológica que soporta el proceso. Esta metodología debe incluir:

- Identificación de los activos de información que se encuentren dentro del alcance del SGSI y las amenazas y vulnerabilidades que los afectan.
- Identificación y valoración del impacto potencial y consecuencias en términos de pérdida de integridad, confidencialidad y disponibilidad de los activos si estos son comprometidos.
- Una metodología para el análisis de la probabilidad de la realización de los riegos de seguridad basado en los controles actuales.
- Establecimiento de un criterio para determinar los niveles de riesgo aceptable.
- Habilidad para reproducir resultados consistentes.

3. Utilizando los objetivos de control y los controles de este documento, el SGSI debe ser capaz de identificar y evaluar los métodos y opciones para el tratamiento del riesgo. Estas opciones incluyen:

    - Aplicar controles que cumplan los objetivos de control y que mitiguen y traten apropiadamente el riesgo.
    - Identificar y entender los riesgos basado en los criterios definidos de análisis de riesgo en el establecimiento del SGSI.
    - Evitar actividades que crean riesgos no aceptables.
    - Transferir riesgos a terceros como aseguradoras.
    - Obtener una aprobación de la alta dirección de los riesgos residuales.

4. El uso del SGSI debe ser aprobado y autorizado por la alta dirección. La documentación del SGSI creado durante el proceso de aprobación debe incluir una declaración de aplicabilidad (SoA, por sus siglas en ingles), el cual detalla todos los controles requeridos para cumplir con los objetivos de control y las razones de su implementación o exclusión. El SoA debe incluir:

    - Los objetivos de control y controles que están o serán implementados, basado en los controles definidos en este documento y las razones de su selección.
    - Una lista de objetivos de control y controles adicionales basados en los requerimientos regulatorios o de negocio.

## 4.2 Hacer: Implementar el Plan del SGSI

Cuando el SGSI ha sido desarrollado y aprobado por la alta dirección, es vital que sea implementado apropiadamente. Para alcanzar dicho objetivo se debe:

1. Formular un plan de tratamiento de riesgo basado en los objetivos de control que identifican las acciones apropiadas, recursos, responsabilidades y prioridades necesarias para gestionar los riesgos de seguridad identificados por el SGSI.
2. Implementar el plan de tratamiento de riesgo con el fin de cumplir con los objetivos de control identificados en esta política o cualquier objetivo de control identificado durante el proceso de implementación del SGSI.
3. Asignar apropiadamente los roles y responsabilidades y proveer los recursos y presupuesto necesario para implementar los controles para cumplir con los objetivos de control del SGSI.

4. Definir un proceso para medir la efectividad de los controles implementados. Este proceso debe ser capaz de producir resultados consistentes.
5. Implementar programas de sensibilización y entrenamiento de seguridad adecuados para garantizar que todos los empleados comprendan sus responsabilidades y tengan el conocimiento necesario para cumplir con los objetivos de control.
6. Documentar e implementar los roles, responsabilidades y procedimientos necesarios para la implementación de controles que garanticen el cumplimiento de los objetivos de control y garantizar que se pueda proveer una detección rápida de los eventos relacionados con la seguridad.
7. Ejecutar una gestión y operación continua del SGSI.

## 4.3 Verificar: Monitorear y revisar el SGSI

El SGSI debe permanecer bajo un monitoreo y revisión constante para garantizar su efectividad en el cumplimiento de los objetivos de control definidos en la planeación del SGSI.

1. Ejecutar monitoreo y revisión de los procesos, procedimientos y otros controles para:

    - Identificar rápidamente cualquier intento o éxito de falencia en seguridad.
    - Proveer a la alta dirección la capacidad de determinar si las responsabilidades de seguridad delegadas al personal o implementadas a través de tecnologías son efectivas para cumplir con los objetivos de control.
    - Determinar si las acciones llevadas a cabo cuando ocurren eventos de seguridad o incumplimientos son efectivas.

2. Actualizar de forma regular el análisis de riesgo para confirmar la validez y el conocimiento de resultados anteriores teniendo en cuenta cambios en los objetivos de negocio, procesos y tecnología.
3. Se debe revisar el SGSI regularmente para validar continuamente si cumple con los objetivos de control, mediante un proceso de cumplimiento de certificación, para identificar áreas potenciales de mejora.
4. El Comité de seguridad de la información debe llevar a cabo auditorías periódicas de la implementación y gestión del SGSI.
5. La gerencia debe revisar el resultado del análisis de riesgo y de otras valoraciones de riesgo como auditorías, proceso de cumplimiento de certificación, adicionalmente a los cambios en ambientes operacionales y otras métricas disponibles que soporten e identifiquen modificaciones del SGSI como cambios en el proceso de análisis de riesgo, planes de tratamiento de riesgo y controles de seguridad.

## 4.4 Actuar: Mantener y Mejorar el SGSI

Para que el SGSI sea efectivo debe someterse a cambios continuos para garantizar que sea actual y que cumpla con los objetivos de control respectivos a los procesos de negocio. Se deben establecer procesos para:

1. Implementar las mejoras, cambios y ajustes al SGSI identificados en la fase de monitoreo y revisión.

2. Modificar las políticas, procedimientos, objetivos de control y documentación basados en las mejoras implementadas.
3. Llevar a cabo las acciones preventivas y correctivas necesarias para eliminar los problemas identificados en el SGSI.
4. Garantizar que las mejoras implementadas cumplan con los objetivos de control.

## 4.5 Requerimientos de documentación

La documentación usada por el SGSI debe ser creada y mantenida apropiadamente.

1. Los documentos deben ser aprobados por la alta dirección para validar su suficiencia y aceptabilidad antes de su implementación.
2. Los documentos deben ser revisados periódicamente, actualizados y reaprobados.
3. Un conjunto de procedimientos y procesos adecuados deben ser implementados para garantizar que los documentos y registros sean protegidos y controlados.
4. Cuando un incidente de seguridad ocurra es importante que se trate en el tiempo y con la prioridad necesaria basada en su severidad. En la mayoría de los casos se requiere evidencia para tratar el incidente de forma apropiada: donde y cuando ocurrió, cuales fueron las circunstancias, la causa, el resultado y el impacto, etc. Un mantenimiento y obtención apropiada de registros de auditoria puede proveer dicha evidencia.
5. Existen requerimientos legales para la recolección y preservación de la evidencia en el caso de incidentes criminales. No solo es importante mantener los registros, sino proteger y mantener la integridad, disponibilidad y confidencialidad de dichos registros.

## 4.6 Resumen de los requerimientos del SGSI

Se debe retener evidencia que soporte el establecimiento, implementación, operación, revisión y mejora continua del SGSI.

1. La alta dirección debe demostrar el compromiso en el establecimiento, implementación y mejora continua del SGSI.
2. La alta dirección debe presupuestar los recursos y las necesidades de entrenamiento para una implementación efectiva del SGSI.
3. El SGSI debe ser revisado y auditado periódicamente con el fin de analizar la efectividad de acuerdo a los objetivos de control. Estas auditorias deben llevarse a cabo de forma objetiva.
4. El SGSI debe someterse a mejoras continuas soportado en la implementación de recomendaciones, acciones correctivas y preventivas basadas en la revisión y auditorias del SGSI.
5. Se debe desarrollar la siguiente documentación:

    - SGSI, incluyendo alcance y objetivos.
    - Declaración de Aplicabilidad (SoA).
    - Procedimientos mandatarios requeridos por la ISO/IEC 27001 para el control de la documentación y registros, auditorias internas del SGSI, acciones correctivas y preventivas.

- Otras políticas y procedimientos que soporten el mantenimiento y desarrollo del SGSI.
- La metodología adoptada para análisis de riesgo.
- Un reporte que presente los resultados del análisis de riesgo llevado a cabo.
- Un plan de tratamiento de riesgo que identifique las acciones a realizar para gestionar los riesgos identificados.
- Procedimientos operacionales que garanticen la implementación efectiva de los controles de seguridad y que demuestre como se mide la efectividad de los controles.
- Registros que provean la evidencia de la implementación de controles.

# 5 Política de Seguridad

**Objetivos de Control:**

- La información y los activos de AREVALO S.A serán protegidos de amenazas que puedan afectar la confidencialidad, integridad o disponibilidad de los procesos de negocio.
- Es necesario que todas las obligaciones legales, regulatorias y contractuales se cumplan.
- El acceso a la información solo será garantizada si las necesidades de negocio lo requieren.
- Todos los usuarios de los sistemas y de los activos de información serán identificados, responsabilizados y monitoreados en el uso de dichos activos.

**Controles:**

## 5.1 Documento de la política de la seguridad de la información

Se debe desarrollar un plan de sensibilización para cualquier nueva práctica de seguridad de la información. El plan de comunicación debe incluir, sin limitar, notificación de nuevas prácticas, integración con la estrategia de sensibilización y, en caso de necesidad, entrenamiento especial para usuarios o personal técnico.

La alta gerencia de AREVALO S.A debe aprobar las políticas de seguridad de la información.

Todas las prácticas y estándares de seguridad deben ser revisados y aprobados por el comité de seguridad de la información.

El Comité de seguridad es el responsable de la revisión y de coordinar la aprobación y la puesta en práctica de cualesquier práctica o estándar de seguridad.

## 5.2 Revisión de la política de seguridad de la información

El Comité de seguridad es el responsable de revisar constantemente la implementación y cumplimiento de las políticas de la seguridad de la información de AREVALO S.A.

Un informe anual de revisión debe ser presentado por el Comité de seguridad e incluir como mínimo un análisis de la aplicabilidad en la práctica de la seguridad a los requisitos actuales de tecnología, negocio y procesos.

Los estándares de seguridad serán revisados por el Comité de seguridad, quien es el responsable de realizar una revisión técnica y asegurar que los estándares se actualicen de acuerdo a las necesidades del negocio y prácticas recomendadas.