




**MANUAL DEL SISTEMA DE GESTIÓN DE
SEGURIDAD DE LA INFORMACIÓN DE
AREVALO S.A**

	MAN-SEG-ARE-20130328		Página 2 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		VERSIÓN 1.0
			FECHA 2013-03-28

Control Documental


Versión	Autor	Fecha	Descripción
1.0	Gustavo Arévalo Arenas	Marzo 26 2013	Versión Inicial

Revisión del Documento

Nombre	Cargo	Versión	Fecha	Comentarios
Gustavo Arévalo Arenas	Gerente de Proyecto	1.0	Marzo 26 2013	Ninguno


Aprobación del Documento

Versión	Aprobación	Fecha	Descripción
Gustavo Arévalo Arenas	Gerente de Proyecto	Marzo 26 2013	Ninguno

	MAN-SEG-ARE-20130328	Página 3 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

CONTENIDO

1	PREFACIO (INTRODUCCION)	4
2	VISIÓN ESTRATÉGICA	5
2.1	Misión de AREVALO S.A	5
2.2	Visión de AREVALO S.A	5
3	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	6
3.1	Principios del Sistema de Gestión Seguridad de la Información "SGSI"	6
3.2	Compromiso de la Dirección	6
3.3	Representante de la Dirección	6
3.4	Alcance Del Sistema De Gestión De La Seguridad De La Información	7
3.5	Exclusiones Del Sistema De Gestión De La Seguridad De La Información	7
3.6	Políticas De Gestión De Seguridad De La Información	8
3.7	Aspectos Relevantes De La Política De Seguridad De La Información	8
3.8	Administración De La Política De SGSI	8
3.9	Alineación De Los Objetivos De Seguridad Con Los Objetivos Estratégicos De Negocio	9
3.10	Roles Y Responsabilidades	11
3.10.1	Comité de Gobierno de Seguridad	11
3.10.2	Comité de Seguridad de la Información	12
3.10.3	Dueño de la Información	12
3.10.4	Oficial de Seguridad	13
3.10.5	Usuario final	14
3.10.6	Custodio de la información	14
3.10.7	Auditoría Interna	15
3.11	Procesos Del SGSI	15
3.12	Obligaciones del poseedor	16
4	GLOSARIO	17


	MAN-SEG-ARE-20130328	Página 4 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

1 PREFACIO (INTRODUCCION)

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.

Cualquier que sea la forma que esta tome ó el medio por el cual es almacenada ó compartida, esta siempre debe ser apropiadamente protegida.

Este manual identifica estos elementos para la gestión de la seguridad de la Información de la Empresa AREVALO S.A, cuyo propósito fundamental es garantizar y propender por la integridad, disponibilidad y confidencialidad, de la seguridad de los sistemas de información y de los datos, definido con base en las directrices y políticas de la Dirección y los requisitos de las normas ISO/IEC 27001:2005 e ISO/IEC 27002:2005.

	MAN-SEG-ARE-20130328	Página 5 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28


2 VISIÓN ESTRATÉGICA

2.1 Misión de AREVALO S.A

Garantizar la prestación de servicios de suministros de productos alimenticios de mar, con un alta estándar de calidad, buscando la satisfacción de nuestros clientes nacionales e internacionales.

2.2 Visión de AREVALO S.A

AREVALO S.A, en el 2018 será reconocida como la Empresa líder en la fabricación y producción de productos alimenticios en Colombia, basados en la prestación de servicios de calidad, con altos estándares internacionales.

	MAN-SEG-ARE-20130328	Página 6 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.1 Principios del Sistema de Gestión Seguridad de la Información “SGSI”

Los principios de seguridad son la base sobre la que se ha definido el Sistema de Gestión de Seguridad de la Información.

- El SGSI soporta la estrategia de la organización.
- El SGSI es un elemento integral para la protección de activos.
- El SGSI debe soportarse en controles Costo-Efectivos.
- Todos los empleados, proveedores y clientes cuentan con una responsabilidad y hacen parte fundamental del SGSI.
- El SGSI debe mejorarse continuamente.


3.2 Compromiso de la Dirección

- Mantener un sistema de gestión de la Seguridad de la Información que garantice el cumplimiento de los objetivos de seguridad requerido para ejecutar los planes estratégicos y los procesos de negocio de AREVALO S.A.
- Garantizar y motivar la participación de todos los funcionarios de AREVALO S.A, proveedores y socios de negocios en el desarrollo del Sistema de Gestión de la Seguridad de la Información
- Mantener un nivel de protección sobre los riesgos que puedan afectar la seguridad de la información que crea, procesa y resguarda la Organización como parte de la debida diligencia de la Dirección.
- Proveer los recursos necesarios para garantizar el debido cuidado de la información que crea, procesa o resguarda la Organización.

3.3 Representante de la Dirección

La Dirección ha designado a la firma UOC-MISTIC como LIDER del proceso de GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, basado en la figura de outsourcing, como su representante frente al sistema de gestión de la seguridad de la información, con la responsabilidad y autoridad para:

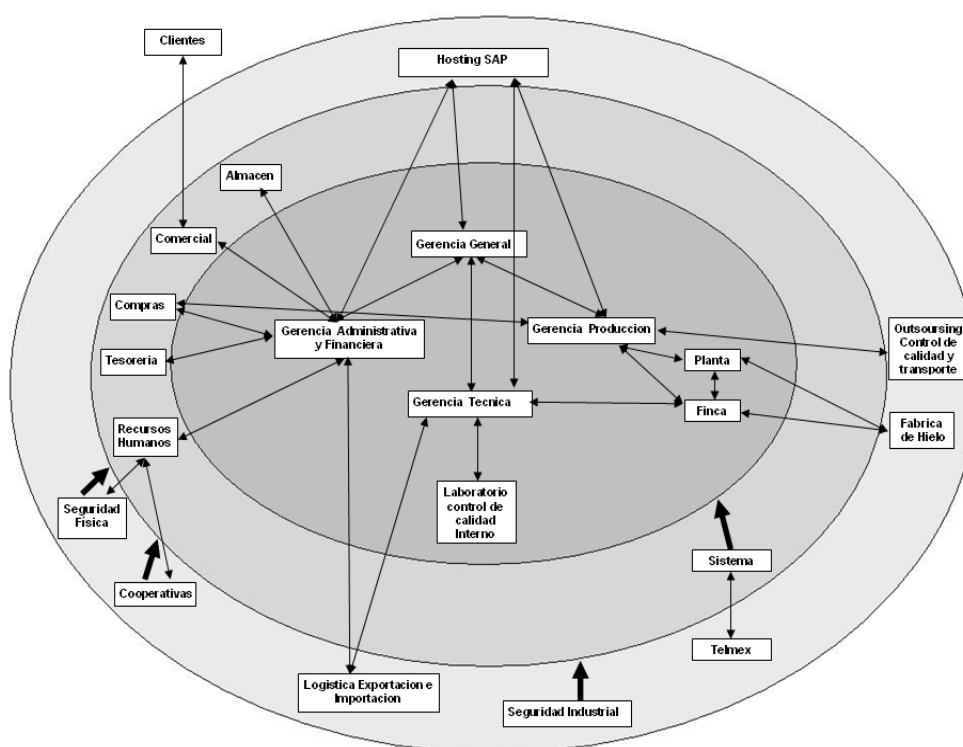
- Asegurar que se promueva la toma de conciencia de la seguridad de la información en todos los niveles de la organización, proveedores y socios estratégicos.

	MAN-SEG-ARE-20130328		Página 7 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		VERSIÓN 1.0
			FECHA 2013-03-28

- Asegurar que se establecen, implementan y mantienen los procesos necesarios para el sistema de gestión de la seguridad de la información.
- Informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información y de cualquier necesidad de mejoramiento.
- Interactuar con partes externas sobre asuntos relacionados con el sistema de gestión de la seguridad de la información.


3.4 Alcance Del Sistema De Gestión De La Seguridad De La Información

El alcance del SGSI definido se presenta en la siguiente ilustración.



El SGSI tiene por alcance todos los procesos de AREVALO S.A (estratégico, misionales y soporte), incluyendo sus activos de información.

3.5 Exclusiones Del Sistema De Gestión De La Seguridad De La Información

	MAN-SEG-ARE-20130328	Página 8 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

El Sistema de Gestión de Seguridad de la Información de AREVALO S.A no excluye ningún numeral de la norma ISO 27001. Para las exclusiones de las mejores prácticas definidas en el estándar ISO 27002 remitirse a la Declaración de Aplicabilidad definida.

3.6 Políticas De Gestión De Seguridad De La Información

El objetivo del SGSI es el de proteger la información que crean, gestionan o resguardan los procesos de negocio con el fin de brindar protección social a través de la prestación de servicios acordes con la propuesta de valor ofrecida, mediante una mejora continua de la seguridad.

Con el fin de cumplir con el objetivo, la organización ha venido trabajando en el diseño de las políticas referentes a la seguridad de la información, las cuales se encuentran en el documento POL-AREVALO-01.

Se deben anexar al contrato de trabajo la aceptación por parte de todos los funcionarios de la organización y a los proveedores se debe exigir la aceptación y conocimiento de la política así como su cumplimiento dentro de las instalaciones o accesos que tengan a AREVALO S.A.

3.7 Aspectos Relevantes De La Política De Seguridad De La Información


- Proteger la privacidad de la información de nuestros clientes.
- Proteger los procesos de creación, procesamiento y resguardo de la información.
- Garantizar que el acceso, intercambio o procesamiento de la información por parte de terceros sea realizada cumpliendo con los más altos estándares de seguridad de la información.
- Asegurarse que la información esté disponible en el momento que los usuarios la requieran.
- Mejorar el costo-eficiencia de los controles de seguridad y su contribución a la rentabilidad del negocio.
- Sensibilizar a los usuarios para garantizar el cumplimiento de las políticas de seguridad.

3.8 Administración De La Política De SGSI

El documento original en medio electrónico reposa en la siguiente dirección electrónica:
<http://AREVALOSA.COM/INTRANET/>

El documento original en medio físico reposa en la oficina de la Gerencia General.

Mantienen copia física controlada de este documento los cargos relacionados en la lista de distribución.

	MAN-SEG-ARE-20130328	Página 9 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28


Quienes se relacionan como poseedores de una copia controlada de este manual en la lista de distribución son informados de sus modificaciones y oficialización vía mail, enviando, y se les orienta sobre la ubicación electrónica del mismo para que pueda ser consultado o impreso en el momento en que se requiera.

El líder del proceso de seguridad de la información, es responsable por la administración de este documento, garantiza la actualización del documento electrónico en la dirección especificada y de las copias físicas controladas que se relacionan en este manual.


EL Líder del proceso así como los directores de AREVALO S.A pueden suministrar copias controladas de este documento por cualquier medio a entidades externas a la organización, previa la autorización por parte del Líder del proceso de seguridad de la información de AREVALO S.A, de tal modo que dicha copia se registre debidamente en el listado de copias controladas para asegurar su permanente actualización.

3.9 Alineación De Los Objetivos De Seguridad Con Los Objetivos Estratégicos De Negocio

ASPECTO ESTRATÉGICO	OBJETIVOS ESTRATEGICOS	OBJETIVOS DE SEGURIDAD
Mercadeo y Producto	1. Consolidar un portafolio integral de servicios alimenticios de productos de mar.	• Asegurar la satisfacción de los usuarios con altos niveles de protección de su información.
	2. Fortalecer la internacionalización de los productos alimenticios de mar.	• Asegurar el uso y desempeño adecuado de los sistemas que crean, procesan o resguardan información.
	3. Consolidar un valioso portafolio de servicios dirigido a las empresas que distribuyan los productos.	• Crear agilidad en el procesamiento seguro de la información.
	4. Desarrollar programas que mejoren la producción de los productos alimenticios.	• Entregar proyectos de seguridad a tiempo y dentro del presupuesto establecido cumpliendo con los estándares de calidad.
	5. Desarrollar el modelo de responsabilidad social empresarial de AREVALO S.A y promover la responsabilidad social empresarial en la región.	• Asegurarse que los procesos de negocio protejan la información de manera rentable, mejora continua y esta lista para cambios futuros.
	6. Promover el desarrollo empresarial de la región	
	7. Promover la cultura de conservación del medio ambiente en la región.	

	MAN-SEG-ARE-20130328	Página 10 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

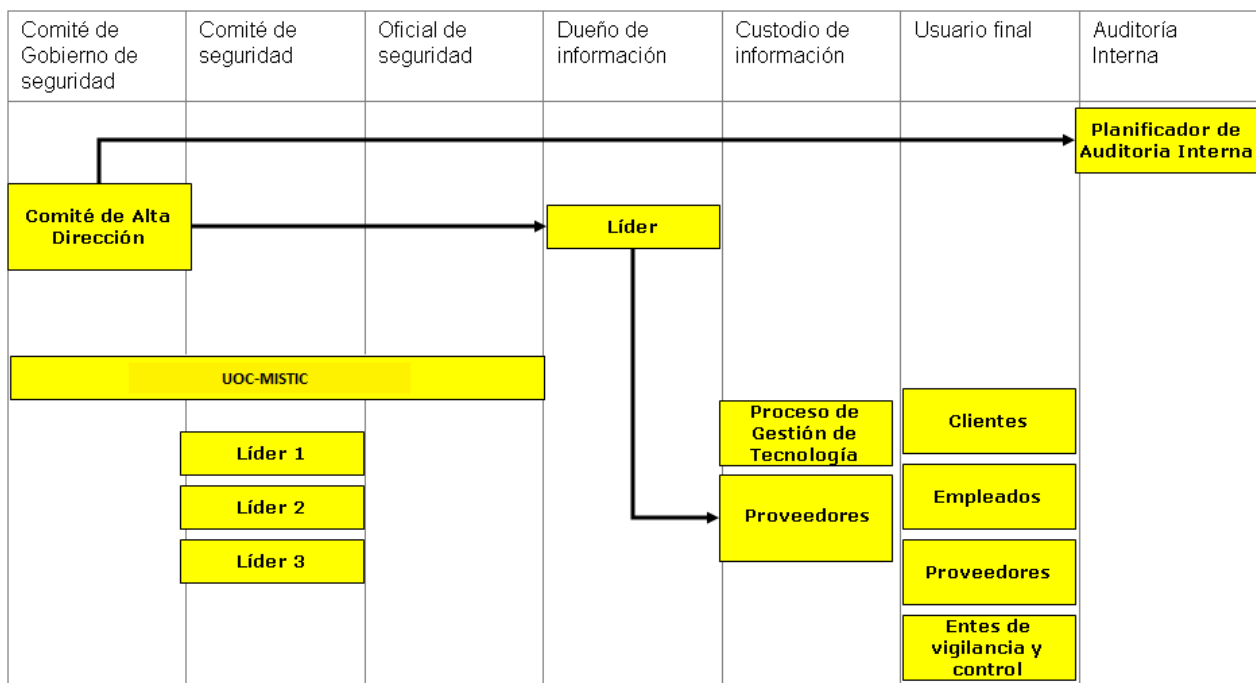
ASPECTO ESTRATÉGICO	OBJETIVOS ESTRATEGICOS	OBJETIVOS DE SEGURIDAD
Diferenciación (Operación)	8. Posicionar a AREVALO S.A como una empresa de alto impacto social.	<ul style="list-style-type: none"> • Establecer controles de seguridad en los procesos de negocio automatizado, efectivo y eficiente. • Adquirir y mantener sistemas de seguridad integrados y estandarizados. • Integrar controles de seguridad aplicables y tecnológicos en procesos de negocio. • Asegurar la satisfacción de los usuarios con altos niveles de protección de su información. • Asegurarse que la información de los procesos esté disponible en el momento que se requieran. • Entregar proyectos de seguridad a tiempo y dentro del presupuesto establecido cumpliendo con los estándares de calidad. • Asegurarse que los procesos de negocio protejan la información de manera rentable, mejora continua y esta lista para cambios futuros. • Responder con los requerimientos de gobernabilidad alineados con dirección de la Junta Directiva. • Establecer claridad del impacto del negocio en las fallas de seguridad de la información.
	9. Desarrollar nuevos productos.	
	10. Optimizar la prestación de los servicios.	
	11. Desarrollar y potencializar la infraestructura física, logística y tecnológica AREVALO S.A.	
Desarrollo de Colaboradores	13. Desarrollar alianzas estratégicas con organismos públicos y privados del orden regional, nacional e internacional.	<ul style="list-style-type: none"> • Establecer y gestionar una estrategia de sensibilización para aumentar las competencias de seguridad que respondan a la estrategia de seguridad de la información.
	17. Garantizar la estabilidad económica de AREVALO S.A.	
	18. Garantizar la consecución de recursos financieros a partir de alianzas y de Cooperación internacional.	
	14. Fomentar la cultura de trabajo en equipo.	
Gestión	15. Propiciar un clima organizacional favorable.	<ul style="list-style-type: none"> • Adquirir y mantener una infraestructura de seguridad integrada y estandarizada.
	12. Desarrollar el sistema de gestión de AREVALO S.A articulado al Sistema de Gestión de la Calidad.	

	MAN-SEG-ARE-20130328	Página 11 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

ASPECTO ESTRATÉGICO	OBJETIVOS ESTRATEGICOS	OBJETIVOS DE SEGURIDAD
	16. Desarrollar el modelo de gestión del talento humano.	<ul style="list-style-type: none"> Asegurar la información proveída en las relaciones con terceros. Mejorar el costo-eficiencia de los controles de seguridad y su contribución a la rentabilidad del negocio.

3.10 Roles Y Responsabilidades

Para gestionar el modelo de seguridad de la información se establecen los siguientes roles y responsabilidades, presentados en la siguiente ilustración.




3.10.1 Comité de Gobierno de Seguridad

Descripción

El comité de gobierno de seguridad debe asistir a AREVALO S.A en todos los temas relacionados con la definición y alineamiento de la estrategia de seguridad, asignación de roles, responsabilidades y niveles de autoridad, gestión y asignación de recursos, validación y gestión de riesgos y en el apoyo para el cumplimiento de los objetivos de negocio.

Responsabilidades

	MAN-SEG-ARE-20130328	Página 12 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

- Aprobar la estrategia de seguridad de AREVALO S.A, con iniciativas tácticas (plan de seguridad) y proyectos que soporten los objetivos de negocio definidos.
- Aprobar el presupuesto de seguridad de la Información y garantizar que los gastos relacionados con seguridad y los proyectos cumplan de forma continua con los requerimientos de negocio.
- Monitorear la estrategia de seguridad, validando su adecuada implementación y recomendando y/o incluyendo nuevos proyectos de seguridad que apoyen el cumplimiento de los objetivos estratégicos.
- Revisar y aprobar las políticas de seguridad o estándares nuevos o modificados.
- Monitorear y evaluar la ejecución de la organización de la seguridad de la información de acuerdo con los indicadores definidos.
- Revisar y modificar las prioridades de las iniciativas de seguridad.
- Revisar y apoyar el presupuesto anual de la organización de la seguridad de la información.

3.10.2 Comité de Seguridad de la Información

Descripción

El comité de seguridad se enfoca en el seguimiento del cumplimiento de tareas tácticas y operacionales de seguridad de la información.

Responsabilidades


- Definir los recursos de seguridad de la información para soportar los requerimientos tácticos, estratégicos y operacionales en las funciones e iniciativas de seguridad.
- Monitorear los planes y proyectos relacionados con seguridad e iniciativas para la entrega de valor, resultados esperados en el tiempo y presupuesto definido.
- Monitorear y revisar los recursos y prioridades que afecten los proyectos de seguridad de la información.
- Gestionar las métricas de seguridad aprobadas por la alta dirección, monitoreando su cumplimiento y el impacto sobre el estado de la seguridad de la información.
- Aprobar los planes proyectados, realizar seguimiento, estimar presupuestos y establecer prioridades y objetivos.
- Desarrollar las políticas de seguridad basado en las mejores prácticas de la industria, los riesgos de AREVALO S.A y de su entorno, y presentarlos al comité de gobierno para su aprobación.
- Establecer guías, estándares y procedimientos operativos que complementen las políticas de seguridad.

3.10.3 Dueño de la Información

Descripción

Es responsable de la información que le sea asignada, así como de su clasificación, control y monitoreo del uso y gestión.

Responsabilidades

	MAN-SEG-ARE-20130328	Página 13 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

- Mantener actualizado el inventario de activos de información de los procesos a su cargo.
- Determinar el nivel de clasificación de la información de la cual es responsable, de acuerdo con su impacto para el negocio y sus objetivos estratégicos.
- Asegurar el cumplimiento de la política de seguridad de la información para garantizar la confidencialidad, la integridad y la disponibilidad de sus activos de información.
- Identificar los riesgos a los cuáles se encuentran expuestos los activos de información a su cargo.
- Definir los controles necesarios para sus activos de información de acuerdo con los niveles de clasificación establecidos y el nivel de seguridad requerido.
- Validar la operación de los controles definidos.
- Aprobar el acceso de empleados y terceros a su información para garantizar que únicamente se realiza cuando sea necesario.
- Monitorear los niveles de acceso de empleados y terceros a su información para garantizar la confidencialidad e integridad.
- Comunicar las novedades de personal a Recursos Humanos con el fin de que se vean reflejadas en los privilegios de acceso de los usuarios a los recursos de información.


3.10.4 Oficial de Seguridad

Descripción

Es el delegado por el Comité de Gobierno de Seguridad de AREVALO S.A para implementar la estrategia de seguridad de la información alineada con los objetivos del negocio, dirigir el programa de seguridad de la información y tomar las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de las políticas y directrices definidas y aprobadas por AREVALO S.A.

Responsabilidades

- Garantizar el alineamiento estratégico de la seguridad de la información con los objetivos de negocio.
- Desarrollar la estrategia de seguridad de la información de AREVALO S.A.
- Supervisar la implementación de la estrategia de seguridad de la información.
- Asegurar el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento continuo del sistema de gestión de la seguridad de la información.
- Asegurar la actualización periódica de la política de seguridad de la información y las directrices y procedimientos que la soportan.
- Asegurar el debido cumplimiento de la política de seguridad de la información de AREVALO S.A.
- Evaluar y aprobar las iniciativas planteadas en función del fortalecimiento del sistema de gestión de seguridad de la información de AREVALO S.A.
- Dirigir el mantenimiento y actualización periódica del inventario de activos de información.
- Dirigir y monitorear la ejecución de evaluaciones de riesgo e impacto al negocio.
- Asegurar la implementación de estrategias adecuadas de tratamiento de los riesgos identificados para los activos de información.
- Definir métricas que permitan monitorear el desempeño del sistema de gestión de seguridad de la información y su valor otorgado a la organización.
- Asegurar la definición y optimización de los recursos asignados al cumplimiento de la estrategia de seguridad.

	MAN-SEG-ARE-20130328	Página 14 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

- Apoyar al Comité de Gobierno de seguridad en la definición de las competencias y habilidades requeridas para los cargos que deben asumir los roles establecidos como parte del gobierno de seguridad de AREVALO S.A.
- Apoyar a los diferentes dueños de la información en la definición y despliegue del programa de conciencia, entrenamiento y educación en seguridad de información.
- Incluir dentro de los planes de entrenamiento de los empleados de AREVALO S.A lo relacionado con seguridad de la información.
- Apoyar el desarrollo de un esquema de sanciones por incumplimiento de las políticas y directrices de seguridad de la información.
- Apoyar al Comité de gobierno de seguridad en la divulgación de las políticas y directrices de seguridad de la información definidas por AREVALO S.A.

3.10.5 Usuario final

Descripción

El usuario final es cualquier empleado, proveedor, contratista, u otra persona autorizada, que utiliza la información de AREVALO S.A en la ejecución de las actividades de su trabajo diario.

Responsabilidades

- Mantener la confidencialidad de la información sensible proveída por la organización para llevar a cabo sus labores diarias.
- Reportar las violaciones a los lineamientos de seguridad definidos por AREVALO S.A al comité de seguridad.
- Aceptar, comprender y aplicar las políticas, estándares y controles técnicos de seguridad de la información de la organización.
- Utilizar la información y recursos corporativos de forma ética, responsable y confidencial.


3.10.6 Custodio de la información

Descripción

El custodio de la información es cualquier empleado, proveedor, contratista, u otra persona autorizada, que tiene la responsabilidad de mantener y/o de soportar los controles de seguridad en los activos de información que contienen la información corporativa.

Responsabilidades

- Garantizar que se cumplan los niveles de servicio definidos.
- Mantener y soportar los controles de seguridad establecidos en el activo para proteger la información.
- Proporcionar asistencia al Dueño de la Información en la selección de soluciones técnicas apropiadas y controles de protección de la información.
- Proveer operativamente el aseguramiento de la Confidencialidad, Integridad y Disponibilidad de la información.

	MAN-SEG-ARE-20130328	Página 15 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

3.10.7 Auditoría Interna

Descripción

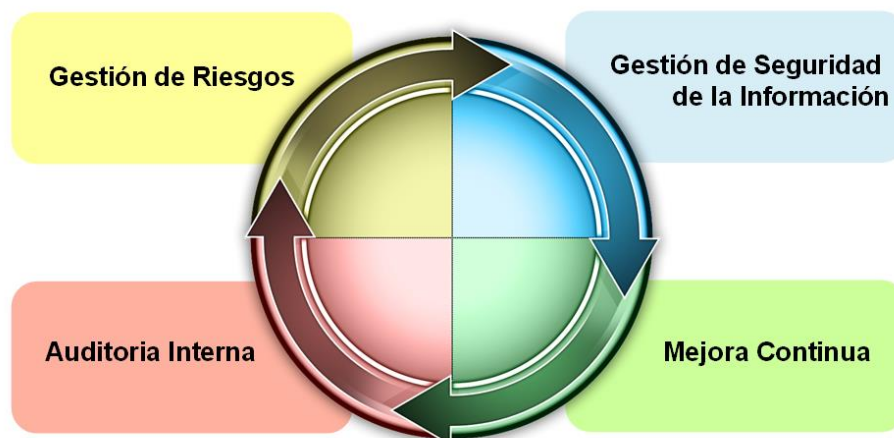
Es encargado de asegurar, de manera independiente, el cumplimiento adecuado de los objetivos establecidos en la estrategia de seguridad de la información de AREVALO S.A. proveyendo seguridad razonable sobre la conservación de los niveles de confidencialidad, integridad y disponibilidad requeridos según la naturaleza e impacto de los activos de información.


Responsabilidades

- Definir procedimientos de pruebas independientes que permitan evaluar el diseño y eficacia operativa de los controles establecidos para proteger los activos de información de AREVALO S.A.
- Emitir recomendaciones para el mejoramiento continuo de los controles establecidos para proteger los activos de información de AREVALO S.A.
- Reportar al Comité de Gobierno de Seguridad las brechas encontradas frente a los objetivos establecidos en la estrategia de seguridad de la información.
- Monitorear la implementación de recomendaciones para el cubrimiento de las brechas identificadas y reportadas
- Revisar el cumplimiento de las políticas y directrices de seguridad de la información definidas por AREVALO S.A.
- Reportar al Comité de Gobierno de Seguridad los casos de incumplimiento de las políticas y directrices de seguridad de la información.

3.11 Procesos Del SGSI

La siguiente ilustración muestra los procesos que soportan el SGSI de AREVALO S.A.



	MAN-SEG-ARE-20130328	Página 16 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

xxxxx Procedimiento de Gestión de Riesgos: Establece las directrices para la identificación, análisis, monitoreo y tratamiento de los riesgos asociados a los procesos y procedimientos definidos para AREVALO S.A.

Xxxxx Procedimiento de Gestión de Seguridad de la Información: El objetivo es proveer los mecanismos adecuados y suficientes para garantizar la confidencialidad, integridad y disponibilidad de la información de la Organización.

Xxxxx Procedimiento de auditoria interna: Definir los lineamientos que deben tenerse cuenta para la planeación y ejecución de auditorías de seguridad de la información de AREVALO S.A, con el propósito de preservar los principios de seguridad (integridad, confidencialidad y disponibilidad) de la información.


Xxxx Procedimiento de Mejora Continua: Establece los puntos que determinan o identifican mejoras al SGSI de AREVALO S.A.

3.12 Obligaciones del poseedor

Este es un documento de uso interno exclusivamente y la duplicación no autorizada del mismo para uso externo se considera como violación al código de ética de la organización, dando lugar a las sanciones que se dispongan para el efecto.

Los líderes de los procesos son responsables por el adecuado uso que se haga de las copias impresas de este manual. Cuentan, como mínimo, con una copia física de este manual, para que pueda ser consultada por los funcionarios a su cargo. Son responsables por asegurar que las copias impresas correspondan en todo momento con la edición vigente.

Todo funcionario que posee una copia de este manual tiene la obligación de consultar si cuenta con la edición vigente del documento previo a la utilización del mismo y, salvo las funciones autorizadas para ello, no está facultado para duplicar bajo ningún mecanismo el documento.

	MAN-SEG-ARE-20130328	Página 17 de 17
	MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	VERSIÓN 1.0
		FECHA 2013-03-28

4 GLOSARIO

- **Activos:** Cualquier cosa que tiene valor para la organización.
- **Disponibilidad:** seguridad de que los usuarios autorizados tiene acceso a la información y a los activos asociados cuando lo requieren.
- **Confidencialidad:** seguridad de que la información no esta disponible o divulgada a personas o entidades o procesos no autorizados.
- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; adicional mente, otras propiedades pueden también ser involucradas tales como autenticidad, registro, no rechazo y credibilidad.
- **Evento de seguridad de la información:** un caso identificado de un sistema, servicio o estado de la red indicando una posible violación de las políticas de seguridad de la información o falla de control, o una situación desconocida nuevamente que puede ser importante en la seguridad.
- **Incidente seguridad de la información:** uno o una serie de eventos de seguridad de la información no esperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Sistema de gestión de la seguridad de la información SGSI:** parte del sistema de gestión global, basada en un enfoque de los riesgos de un negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Integridad:** protección de la exactitud y estado completo de los activos.
- **Riesgo residual:** nivel restante de riesgo después de que se han tomado medidas de tratamiento de riesgo.
- **Aceptación del riesgo:** decisión de asumir el riesgo.
- **Análisis de riesgo:** uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Valoración del riesgo:** proceso global de análisis y evaluación del riesgo.
- **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra el criterio de riesgo establecido para determinar la importancia del riesgo .
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Tratamiento de riesgo:** proceso de selección e implementación de medidas para modificar el riesgo.
- **Declaración de aplicabilidad:** documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.