Política de Seguridad de Información

Firmantes

Nombre	Fecha	Firma
Luis Carlos Astaiza *Gerente*		
Diego Arbey Dorado Cruz *Talento Humano*		
Jessika Johana Astaiza Cajas *Departamento Jurídico*		
Nombre firmante *cargo*		

Historial

Fecha	Razón de cambio (s)	Autor(es)

Índice

Alcances

Las políticas de seguridad de la información se aplican a toda información obtenida, creada, manipulada o administrada por **AEES SYSTEM SAS**, dentro de sus Recursos de Información y sus procesos Core de la empresa. Estas políticas y estándares están basadas en la interpretación del estándar ISO 27001, y otros materiales de referencia, y se aplican igualmente a todos los niveles de gerencia y en general a todo el personal. Adicionalmente, esta Política se aplica a toda la información generada por las funciones, procesos y procedimientos que involucren recursos de Información de **AEES SYSTEM SAS**, durante el tiempo de transferencia hacia un agente externo de la organización o durante su propia disposición y destrucción.

Audiencia

Estas Políticas se aplican igualmente a todo el personal de y a todos los otros usuarios externos autorizados a acceder a los recursos de Información de **AEES SYSTEM SAS**.

Definiciones

Información: Toda información, independientemente de su forma, que es creada, almacenada o procesada por los recursos de información, redes de comunicaciones y datos o medios de almacenamiento.

Recursos de Información (RI): Todo equipo de cómputo, impresiones, recursos en línea, medios de almacenamiento magnético y todas las actividades relacionadas a sistemas de cómputo, incluyendo cualquier dispositivo capaz de recibir e-mails, navegación en la Web, o con capacidad de recepción, almacenamiento, manejo, o transmisión electrónica de datos, por ejemplo y no limitado a, servidores, computadores personales, computadores portátiles, computadores de mano, asistentes personales portátiles (PDA), pagers o beepers, Smart phone, sistemas de procesamiento distribuido, redes de datos, recursos de telecomunicación, teléfonos, equipos de fax e impresoras. Adicionalmente, son considerados como Recursos de Información: los procedimientos, los equipos, instalaciones físicas, software, y data que sean diseñados, producidos, operados y mantenidos para crear, recolectar, grabar, procesar, almacenar, recuperar, desplegar y transmitir información.

Aplicación de las Políticas

AEES SYSTEM SAS, protegerá todos sus Recursos de Información de la organización de acuerdo con las políticas definidas.

Específicamente, la organización aplicará políticas, procedimientos, buenas prácticas, estándares, y guías para proteger las funciones de los RI de datos internos, errores de programación, mal manejo por individuos dentro de o fuera de la empresa. Esto con la finalidad de proteger a la organización de riesgos que comprometan la integridad de los programas, violación de los derechos individuales a la privacidad y confiabilidad, violación del derecho penal, o de potenciales daños a la seguridad pública.

Todos los Programas de seguridad de los recursos de información de la organización serán responsables y adaptables a los cambios tecnológicos que afecten los Recursos de Información.

Violaciones

Cualquier evento que resulte en robo, pérdida o uso desautorizado, declaración no autorizada, modificaciones desautorizadas, destrucciones desautorizadas, o acceso a RI denegados, constituyen una brecha de seguridad y a su confidencialidad. Estas violaciones pueden incluir, pero no limitarse, a los siguientes:

- Exponer a la organización a actuales o potenciales pérdidas monetarias comprometiendo la Seguridad de los RI.
- Involucra las declaraciones de información sensible o confidencial o el uso no autorizado de datos o recursos de la organización.
- Incluye el uso de los RI para beneficio personal, no ético, dañino o con propósitos ilícitos.

Acciones Disciplinarias

La Violación de estas Políticas pueden resultar en acciones disciplinarias inmediatas, pero no limitadas a:

- Reprimendas Formales,
- Suspensión o acceso restringido a los Recursos de Información de la institución
- Restitución o indemnización por cualquier daño o apropiación ilícita de cualquier propiedad de la institución,
- Suspensión sin pago,
- Término de empleo,
- Término de contrato,
- Despido,
- Proceso Civil, o
- Proceso Penal.

Roles y Responsabilidades

Área de tecnología: Área responsable de la gestión y administración de los recursos de información de **AEES SYSTEM SAS**, La designación del Área de Sistemas está dirigida a establecer la responsabilidad de diseñar e implementar políticas para el manejo de los recursos de información, proveer una mejor coordinación de las actividades que involucren acceso, procesamiento y administración de la información dentro de la organización, y para asegurar una mejor orientación de tales actividades dentro y fuera de la misma. El área de tecnología tiene la autoridad y responsabilidad para implementar Políticas de Seguridad, Procedimientos, Prácticas Estándares y Guías para proteger los Recursos de Información de la empresa.

Propietario: Es el gerente, director o usuario responsable de las funciones que tiene que ver con el manejo y soporte de los recursos, las personas a los cuales se les responsabiliza de llevar a cabo los programas que utilizan los recursos de información. El propietario es responsable de establecer los controles que provean la seguridad. Dependiendo sea el caso, la propiedad puede ser compartida por gerentes o directores de diferentes departamentos.

Usuario: Tiene la responsabilidad de (1) usar los recursos sólo para los propósitos establecidos por el propietario y la organización, (2) cumplir con los controles establecidos por el propietario y la organización, y (3) prevenir declaraciones de información confidencial o sensible. El usuario es la persona que ha sido autorizada para leer, ingresar o actualizar información por el propietario de la información. El usuario cumple el más simple control efectivo para proveer adecuada seguridad.

Políticas Estándar Referencias	Detalle Basado en las Mejores Prácticas
1	Los controles de Seguridad de los RI no deben ser obviados o inutilizados.
2	La conciencia de seguridad del personal debe ser continua, reforzada, actualizada y validada.
3	Todo el personal es responsable por el manejo y del uso de los RI y son responsables por los actos relacionados a la seguridad de los RI. El personal es igualmente responsable de reportar cualquier sospecha o confirmación de violaciones o manejo inapropiado de las políticas de seguridad de información.
4	Las contraseñas, números de identificación de personal (PIN), claves de seguridad (tarjeta inteligente de seguridad), y otros procedimientos y dispositivos de seguridad en los sistemas de informáticos deben ser protegidos por el usuario. Toda violación de seguridad debe ser reportada al responsable o gerente encargado y/o al área de Sistemas.
5	El Acceso a, el cambio y el uso de los RI deben ser estrictamente seguros. La autorización para acceso a la información para cada usuario debe ser revisada regularmente, así como el cambio de status del trabajador como: transferencia, promoción, baja o culminación de sus actividades.
6	El uso de los RI debe ser oficialmente autorizado, los mismos que son sólo para propósitos de la empresa. No existe garantía de privacidad personal o acceso a herramientas, pero no limitada a; e-mail, navegación en Internet, y otras herramientas de discusión electrónica. El uso de estas herramientas de comunicación electrónica puede ser monitoreadas para realizar o esclarecer reclamos o procesos de investigación. Los departamentos o áreas que tienen a cargo el manejo de computadores deben ser responsable de la adecuada utilización de los RI, el efectivo manejo del mismo, y de reportar su estado y manejo.
7	Cualquier información utilizada en un sistema de los RI, debe ser mantenida con confidencialidad y seguridad por el usuario. El hecho de que la información sea almacenada electrónicamente no cambia el requerimiento de mantener la información segura y confiable. Más bien, el tipo o clasificación de la información por sí misma es la base para determinar si la información debe guardarse en forma confidencial y segura. Adicionalmente, si esta información es almacenada en un papel o un formato electrónico, o si la información es copiada, impresa o

trasmitida electrónicamente debe ser protegida como confidencial y segura.

Políticas Estándar (continuación) Referencias	
8	Al término de la relación de trabajo con la institución, los usuarios deben entregar todos los bienes y RI asignados por la institución. Se deben aplicar todas las políticas de seguridad de los RI y relacionadas con el evento de culminación de relaciones laborales hasta que la devolución sea realizada. Asimismo, esta política da por terminada toda relación.
9	El propietario debe comprometer al Gerente del Área de tecnología y recibir su aprobación, a la elaboración de cualquier proyecto de adquisición de hardware, compra o desarrollo de software para la organización. Los costos de las adquisiciones, desarrollo y operación del hardware y aplicaciones deben ser autorizados por los Gerentes o directores apropiados. La Gerencia y los departamentos solicitantes deben actuar dentro de sus límites de aprobaciones de acuerdo con las políticas de autorización de compras de la organización.
10	El departamento o área que requiera o autorice una aplicación de computador, debe cumplir con los pasos apropiados para asegurar la integridad y seguridad de todos los programas y archivos de información creados u obtenidos por las aplicaciones de cómputo.
11	La red de RI es de propiedad y controlada por el área de tecnología. Las aprobaciones deben ser obtenidas del Área de Sistemas y tecnología antes de conectar a la red un recurso que no cumpla con las guías o estándares de la red publicados. El área de Sistemas se reserva el derecho de remover de la red cualquier recurso que no cumpla con los estándares o que no sean considerados como adecuadamente seguros.
12	La venta o alquiler de aplicaciones de cómputo o datos, incluyendo lista de e-mail y directorios telefónicos, a otras personas o organizaciones debe cumplir con todas las políticas y procedimientos legales y fiscales de la organización y las leyes nacionales existentes.
13	La integridad del uso general de software, utilidades, sistemas operativos, redes y archivos de información, son responsabilidad década uno de los departamentos o áreas en que se encuentra dividida la empresa. Los datos para pruebas y con propósitos de investigación deben ser autorizados por el Gerente del Área de tecnología.

14	Todos los cambios o modificaciones en los sistemas de RI, redes de datos, programas o datos deben ser aprobados por el departamento encargado el cual es responsable de su integridad.

Políticas Estándar (continuación) Referencia

15	El área de tecnología debe proveer los controles de acceso adecuados para monitorear los sistemas y proteger la información y programas de malos manejos de acuerdo con las necesidades definidas por los propietarios o usuarios. El acceso debe estar correctamente documentado, autorizado y controlado.
16	Todos los departamentos o áreas deben evaluar cuidadosamente los riesgos de cambios desautorizados, declaraciones desautorizadas, o pérdida de los datos de los que son responsables, y asegurar a través del uso de sistemas de monitoreo, que la organización esté protegida contra daños u otros. El propietario de las aplicaciones y el área de Información y tecnología deben contar con un backup apropiado y planes de contingencia para así contrarrestar desastres o riesgos de daños o perjuicios basados en los requerimientos de la organización.
17	Todos los contratos de sistemas o aplicaciones de cómputo, alquiler, licencias, u otros acuerdos deben ser autorizados y firmados por el gerente y el Área de tecnología y/o usuario autorizado de la organización, y debe contener los términos aprobados por el departamento legal, notificando a los proveedores o contratistas para los RI de la organización, el respetar los derechos de propiedad de los sistemas de información, programas, y datos requeridos.
18	Los sistemas de cómputo de los RI y equipos asociados, utilizados para los fines de la organización, y que son operados y administrados fuera del control de la empresa, deben cumplir requerimientos contractuales y estar sujetos a monitoreo.
19	El acceso externo desde y hacia los RI deben cumplir las guías de seguridad apropiadas y publicadas por la organización.
20	Todo software comercial utilizado en los sistemas de cómputo debe contar con acuerdos de licencias de software, que describa los derechos de uso y las restricciones del producto. El personal debe cumplir con todas los acuerdos de licencias y no debe realizar copias ilegales del software. El área de tecnología

	se reserva el derecho de remover cualquier software sin licencia de los RI.
21	El área de tecnología se reserva el derecho de remover cualquier software o archivos de cualquier sistema de cómputo, no relacionado con el negocio o fines de la organización. Ejemplos de este software son: juegos, programas instant messengers o chat, pop e-mail, archivos de música, fotos, freeware y shareware.
22	Las adherencias a todas las otras políticas, prácticas estándar, procedimientos y guías utilizadas, como soporte de esta política de Seguridad de Información, es obligatoria.

Asistencia	Cualquier solicitud relacionada con esta política o la aplicación de esta debe ser referida al Gerente de la empresa o al área de tecnología.
Referencias	ISO 27001 Estándar Revisión de Estándares y Publicación de Recomendaciones.