


CIRCULAR ASUNTO: POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
CÓDIGO: CIR-375	ÁREA GERENCIA DE RIESGOS	EMISORA:	FECHA:	
VERSIÓN: 2	CREA <input type="checkbox"/> MODIFICA <input checked="" type="checkbox"/> MANUAL <input type="checkbox"/> NORMA <input checked="" type="checkbox"/> PROCEDIMIENTO <input type="checkbox"/>			
Documento de Uso Interno				

PARA:

Toda la Compañía.

OBJETIVO:

Definir política y normas para la incorporación de medidas de seguridad de la información y ciberseguridad en los procesos de Planeación y Proyectos TI, Infraestructura y Servicios Tecnológicos y Mantenimiento de Sistemas de Información, ya sean propiedad de Previsora o administrados por terceros.

DOCUMENTACIÓN RELACIONADA:

- DOCUMENTO DE LINEAMIENTOS DE SEGURIDAD PARA APLICACIONES Y SERVICIOS.
- CONTROL DE CÓDIGO FUENTE.

ALCANCE:

La política descrita a continuación aplica para todos los sistemas de información y/o componentes tecnológicos de Previsora S.A. Las directrices de la Política de Adquisición, desarrollo y mantenimiento de los sistemas de información son aplicables a los procesos: Planeación y Proyectos TI, Infraestructura y Servicios Tecnológicos y Mantenimiento de Sistemas de Información.

REQUERIMIENTOS REGULATORIOS

La Política de Seguridad de la Información para la Adquisición, Desarrollo y Mantenimiento de Sistemas de PREVISORA S.A, busca el cumplimiento de los requerimientos regulatorios aplicables de las circulares emitidas por la Superintendencia Financiera de Colombia, la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013.

NORMAS INTERNACIONALES APLICABLES

De conformidad con los requerimientos de la Superintendencia Financiera de Colombia (SFC), PREVISORA S.A., define como base metodológica el modelo conceptual de la Norma ISO/IEC 27001 e ISO 27032

POLÍTICA

Establecer que la seguridad de la información y la ciberseguridad sean una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas, servicios web y apps que procesan información confidencial de la compañía o de los consumidores financieros.

Los lineamientos aquí listados han sido ratificados por el Comité de Seguridad de la Información.

NORMAS

a) Responsabilidades

- I. Todos los sistemas de información (aplicaciones o servicios), que sean desarrollados o implementados por PREVISORA S.A., y/o por terceras partes, deben cumplir con requerimientos básicos de seguridad de la información y de ciberseguridad, los cuales serán definidos por el Oficial de Seguridad de la Información y el Oficial de Seguridad Informática de la entidad, conforme a los resultados de los análisis de riesgo que se realicen en conjunto con los dueños del activo de información que hayan sido designados.
- II. El Custodio de los Activos de Información de PREVISORA S.A., asociados a los sistemas de información (aplicaciones o servicios) y/o sus componentes tecnológicos, es la Gerencia de Tecnología de la Información.
- III. Los propietarios de los activos de información deben considerar la definición de los requerimientos de seguridad en las etapas tempranas del ciclo de desarrollo de los sistemas de información y/o de los proyectos de implementación, con el fin de mantener la confidencialidad, integridad y disponibilidad de los mismos. Es responsabilidad del custodio del activo de información la incorporación y mantenimiento de los controles que se hayan definido para su puesta en ambientes de producción.
- IV. Cada propietario de un activo de información que esté relacionado con los sistemas de información (aplicaciones o servicios) de PREVISORA S.A., debe definir los registros de auditoría que a nivel de aplicación deben ser necesarios activar. Los aspectos de auditoría de los sistemas de información deben ser mejorados considerando los resultados de las auditorías realizadas.
- V. Es responsabilidad del Custodio de los Activos de Información de PREVISORA S.A., asociados a los sistemas de información (aplicaciones o servicios) y/o sus componentes tecnológicos, evaluar e implementar los requerimientos de auditoría solicitados. En caso que técnicamente no sea viable, debe quedar constancia del análisis realizado y/o propuesta de una alternativa que compense lo requerido.

b) Seguridad en Aplicaciones – Desarrollo Seguro

- I. Todos los sistemas de información (aplicaciones o servicios) de la compañía deben contar con mecanismos de control de acceso y herramientas de gestión de usuarios.
- II. Todos los sistemas de información (aplicaciones o servicios) de la compañía deben realizar procesos de autenticación soportados por matrices de acceso que limiten los perfiles a actividades de consulta, modificación, población, parametrización, y/o procesamiento de la información que allí se encuentre disponible.
- III. Las matrices de acceso para los sistemas de información (aplicaciones o servicios) de la compañía, deben ser definidas por los dueños de los aplicativos y custodiadas por el Oficial de Seguridad de la entidad.
- IV. Los sistemas de información (aplicaciones o servicios) deben ejercer control sobre los datos que son ingresados, validando características mínimas como longitud, coherencia, y el tipo de dato.
- V. Los datos de salida de los sistemas de información (aplicaciones o servicios) deben ser procesados, y validados a través de las reglas y procesos de negocio definidos y avalados por el dueño del activo.
- VI. El procedimiento de gestión de cambios que contemple las actividades de implantación, desarrollo, soporte y mantenimiento de los sistemas de información (aplicaciones o servicios), debe incluir actividades para la revisión y evaluación de riesgos de seguridad y de ciberseguridad y por ende la definición e inclusión de controles de seguridad. Los cambios que se desarrollen en los sistemas de información (aplicaciones o servicios) deben ser aprobados por los dueños de los activos de información involucrados.
- VII. Se debe establecer un protocolo que permita realizar la revisión del correcto funcionamiento de los sistemas de información cuando se ejecutan cambios en este, o en alguno de los componentes que los soportan, , teniendo en cuenta lo establecido por la Gestión de Cambios de la Previsora.
- VIII. Los contratos con terceros para el desarrollo de software deben considerar los siguientes requerimientos mínimos:
 - a. Definición de Acuerdos de Servicio.
 - b. Desarrollo de software cumpliendo la guía OWASP (Open Web Application Security Project) u otra metodología de calidad en el desarrollo de software considerada como mejor práctica
 - c. Definición, integración e implementación de las estrategias de continuidad / recuperación.
 - d. Disponibilidad de Auditorías por parte de PREVISORA S.A., a los procesos de desarrollo de software.
- IX. El custodio de los Activos de Información de PREVISORA S.A., asociados a los sistemas de información (aplicaciones o servicios), debe realizar revisiones periódicas o evaluaciones para la identificación de vulnerabilidades sobre los sistemas de información de PREVISORA S.A. Dichas actividades deben incluir planes de mejora y/o remediación.

- X. Se debe evitar la realización de cambios no autorizados a datos en los sistemas en producción. En caso que se requiera, el funcionario que lo necesite, debe realizar el trámite de la autorización con el propietario del activo de información, a través del procedimiento establecido por la Gerencia de Tecnología.
- XI. Se debe contar con la separación de los ambientes de desarrollo, pruebas y producción para los casos en los que aplique, para los casos en los que no aplique dicha separación o no sea posible su implementación deberá quedar por escrito la aceptación de los mismos desde la fase de construcción e incluir el análisis de riesgos de no contar con dichos ambientes.
- XII. Se debe controlar estrictamente el acceso a los códigos fuente de programas y elementos asociados (tales como diseños, especificaciones, planes de verificación y planes de validación), con el fin de evitar la introducción de funcionalidad no autorizada y para evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual y mantener un inventario actualizado de los códigos fuente de programas y elementos asociados.
- XIII. Los dueños de los activos de información deben definir si debido a la sensibilidad de la información, se requiere del uso de técnicas de cifrado de datos para su transmisión.

c) Recursos

- I. PREVISORA S.A., se compromete a brindar el recurso humano, técnico y económico necesario para que el modelo de Seguridad de la Información plasmado en esta política se implemente, opere, mantenga y mejore.
- II. La Alta Dirección de PREVISORA S.A. se compromete a proveer los medios necesarios para que los procesos de la Compañía clasifiquen, den tratamiento y actualicen la matriz de activos de información del proceso.

d) Revisión

- I. Esta política se encuentra inmersa en el proceso de mejora continua del Sistema de Gestión de Seguridad de la Información, por tal razón se revisará cuando sea requerido conforme los cambios organizacionales que se den en el transcurso del tiempo o en su defecto una vez cada dos años.
- II. Las políticas, normas y procedimientos de seguridad de la información deben ser revisados cuando se den cambios en los procesos de la Compañía que ameriten dicha revisión o cuando el Comité o el Oficial de Seguridad de la Información así lo definan. Esta actividad debe ser coordinada por el Oficial de Seguridad de la Información.

e) Manejo de Excepciones

Las excepciones a cualquiera de las directrices de la Política de Seguridad General o sus políticas derivadas (como la presente), serán admitidas únicamente cuando el Oficial de Seguridad de la Información avale y divulgue su aceptación. Las excepciones a los lineamientos existentes deben estar sustentadas sobre la base de un análisis de riesgos aplicable.