PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION PARA LA UNIVERSIDAD DEL ATLÁNTICO

OFICINA DE INFORMÁTICA

SISTEMA INTEGRADO DE GESTIÓN

TABLA DE CONTENIDO

Contenido

INTRODUCCION

El Plan de seguridad y privacidad de la información es un documento estrategico que aborda la necesidad de un sistema de gestión para la seguridad de la información en el proceso de Gestión Tecnológica y Comunicaciones en la Universidad del Atlántico. Para la mejora de esta gestión es necesario transmitir a la comunidad universitaria niveles de concientización, compromiso y prevención en el buen uso de los recursos públicos con base en la legislación y normatividad vigente referente a la Seguridad de la Información.

La Universidad del Atlántico implementa las mejores prácticas de la seguridad de la Información con base en el análisis de la misión, visión, metas institucionales y el Manual de Seguridad y Políticas de Informática con el fin de tomar acciones para el mejoramiento continuo, protección de los activos de información para minimizar riesgos que afecten la continuidad de la institución.

En el presente anexo se muestra la política de seguridad de la información.

1. POLITICA

La Alta dirección de la **UNIVERSIDAD DEL ATLÁNTICO**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un **Sistema de Gestión de Seguridad de la Información** buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de nuestra institución. Para la **UNIVERSIDAD DEL ATLÁNTICO** la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con el objeto de mantener un nivel de exposición que permita responder por altos niveles de confiabilidad, integridad y disponibilidad en los sistemas de información al servicio de la comunidad universitaria y grupos de interés, mediante la implementación de estándares internacionales de seguridad de información y buenas prácticas.

El establecimiento, implementación, mantenimiento y mejora continua de la Política de Seguridad de la Información garantiza un compromiso y concientización ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad logrando la mejora continua en los procesos acorde al Plan Estratégico Institucional.

La Política de Seguridad de la Información en el proceso de Gestión Tecnológica y Comunicaciones es la declaración general que representa la posición de la administración de la UNIVERSIDAD DEL ATLÁNTICO con respecto a la protección de los activos de información (personas, procesos y las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información apoyado las normativas vigentes, políticas y manuales para la seguridad de la información.

2. OBJETIVO

La Universidad del Atlántico, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a los valores institucionales, establece la función de Seguridad de la Información en la Institución, con el objetivo de:

- Brindar orientación y soporte, por parte de la alta dirección, para la seguridad de la información de acuerdo con los requisitos de la institución y con las leyes y reglamentos pertinentes

- Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la institución

- Asegurar que los funcionarios, contratistas y proveedores comprenden sus responsabilidades, sean idóneos en los roles asignados, cumplan sus compromisos de la seguridad de la información, protegiendo los intereses de la institución como parte del proceso de actualización o terminación de empleo o contrato

- Identificar y asegurar los activos de información organizacionales y definir las responsabilidades de protección apropiadas, de acuerdo con su importancia para la institución

- Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios

- Garantizar la seguridad de las operaciones controlando y documentando los cambios institucionales, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afecten la seguridad de la información

- Mantener la seguridad de la información en el proceso de Gestión Tecnológica y de Comunicaciones, estableciendo políticas, procedimientos y controles de transferencia formales en la institución y las partes externas

- Asegurar que la seguridad de la información sea 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 publicas

- Mantener el nivel acordado de seguridad en la información y protección de los activos de la institución con los proveedores

- Mantener e incrementar los niveles de confianza de la comunidad universitaria, clientes, proveedores y grupos de interés

- Garantizar la continuidad de la actividad de la institución frente a incidentes

- Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación, contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad

3. ALCANCE

El presente documento es de aplicación a toda la comunidad universitaria, dependencias que componen la institución, a sus recursos, a la totalidad de los procesos internos o externos vinculados al proceso de Gestión Tecnológica y de Comunicaciones, a través de contratos o acuerdos con terceros y a todo el personal de la Universidad del Atlántico y la ciudadanía en general, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Las responsabilidades frente a la seguridad de la información serán definidas, difundidas, publicadas y aceptadas por la comunidad universitaria.

La Universidad del Atlántico protegerá la información generada, procesada o resguardada por el proceso de Tecnología y Comunicaciones, Servicio TI y activos de información estableciendo controles a los riesgos que se generan de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

La Universidad del Atlántico protegerá la información creada, procesada, transmitida o resguardada por sus procesos de la organización, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es

fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La Universidad del Atlántico protegerá su información de las amenazas originadas por parte de las personas vinculadas (Administrativos, docentes, contratistas y otros) y con compromisos contractuales con la institución

- La Universidad del Atlántico protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos

- La Universidad del Atlántico controlará la operación de sus procesos institucionales garantizando la seguridad de los recursos tecnológicos y las redes de datos

- La Universidad del Atlántico implementará control de acceso a la información, sistemas y recursos de red

- La Universidad del Atlántico garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información

- La Universidad del Atlántico garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora continua y efectiva de su modelo de seguridad

- La Universidad del Atlántico garantizará la disponibilidad de sus procesos institucionales y la continuidad de su operación basada en el impacto que pueden generar los incidentes

- La Universidad del Atlántico garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

4. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

La Universidad del Atlántico garantiza el liderazgo y compromiso al cumplimientos de los requisitos según la norma ISO/IEC 27001:2013 en el proceso de establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada ***Comité Gestor de Seguridad de la Información*** cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- **Rector** (Director CEO, Representante Legal) o un delegado
- **Secretario General** o un delegado
- **Vicerrector de Docencia** o un delegado
- **Vicerrector Administrativo** o un delegado
- **Jefe de la Oficina de Planeación** o un delegado
- **Jefe de la Oficina de Informática** (Director CIO) o un delegado
- **Jefe Talento Humano**
- **Jefe de Jurídica**
- **Asesor certificado en Seguridad de la Información**

Este comité, deberá revisar y actualizar anualmente la política de seguridad de la información, presentando las propuestas acordes al plan estratégico institucional para su futura aprobación mediante resolución o acto jurídico correspondiente. Las funciones del Comité Gestor de Seguridad de la Información son:

- Establecimiento, implementación, mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información

- Establecer la Política de seguridad de la información y los objetivos de la seguridad de la información

- Asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos del Sistema Integrado de Gestión SIG

- Asegurar los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles

- Asegurar que el sistema de gestión de la seguridad de la información logre los resultados previstos

- Comunicar la importancia de una gestión de seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de seguridad de la información

- Promover la mejora continua

5. RESPONSABILIDADES

Los propietarios de los riesgos.
Previa identificación y valoración de sus activos de información, hacen parte de los líderes de procesos que son responsables de Seguridad de la Información en sus dependencias, oficinas y entornos a su cargo, por lo tanto ***deben*** seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías, manuales y procedimientos recomendados por el Comité Gestor de Seguridad de la Información y aprobados por la Alta Dirección.

El **Coordinador del Comité de Seguridad de la Información.**
Será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política. Convocar y presidir las reuniones del Comité Gestor de Seguridad de la Información.

Equipo de Planificación de Seguridad de la Información.
Durante el establecimiento y creación del Comité Gestor de Seguridad de la Información se conformará un equipo de Líderes del SGSI y el CIO que trabajarán entre departamentos y resolverán conflictos relacionados con la seguridad de la información.

Los Líderes de Procesos.
Responsables de Seguridad Informática Responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad, está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité Gestor de Seguridad de la Información.

Los Propietarios de los Riesgos.
Son responsables de la clasificación, mantenimiento y actualización de los sistemas de información; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener acceso a la información de acuerdo a sus perfiles, funciones y competencia. En general, tienen la responsabilidad de mantener la integralidad, confidencialidad y disponibilidad de los activos de información durante su ciclo de vida.

Jefe de Talento Humano.
Cumplirá la función de notificar a todo el personal que se vincula contractualmente con la Universidad del Atlántico, de las obligaciones, acuerdos y compromisos respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, instructivos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de las actualizaciones que en ella se produzcan a todo el personal, a través de acuerdos de *Confidencialidad* y de tareas de capacitación, sensibilización continua en materia de seguridad según lineamientos dictados por el Comité Gestor de Seguridad de la Información.

Jefe de la Oficina de Informática.
Debe seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la entidad.

Corresponde a dichas jefaturas determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el **Jefe de Bienes y Suministros** y el **Jefe de Servicio Generales (Recursos Físicos)**.

Jefe de la Oficina Jurídica.
Verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Así mismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Oficina de Control Interno.
Es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas

de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

Líder Ético Ambiental.
Miembro de la comunidad universitaria (Estudiante, docente, administrativo u otros) interesado en motivar a otros individuos del entorno universitario, al objetivo de configurar una cultura ética institucional y hacer promoción de la Seguridad de la Información y proyectos integrales acordes al Plan de Acción Ético institucional.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

Personal de la Universidad.
Todo el personal de la Universidad del Atlántico, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por la **Oficina de Informática**, en cuanto a la información y **la red de datos** , en cuanto a los dispositivos hardware y los elementos de software.

El Estatuto General y el Estatuto Docente deben contemplar procesos y sanciones disciplinarias para los casos en que se presente usos inadecuados de información y TI que violen los términos y condiciones.

La **Oficina de Talento Humano** junto con la **Oficina de Informática** se encargará de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

La **Oficina de Informática** en conjunto con la **Sección de Biblioteca** se encargará de crear y mantener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, delitos informáticos entre otros.

Estudiantes.
Para poder usar los recursos de TI de la Universidad del Atlántico, los estudiantes deben poseer matricula financiera y académica, conocer y aceptar en cada matrícula

de semestre un acuerdo con los términos y condiciones en cuanto a seguridad y política de protección de datos personales sensibles. La **Oficina de Informática en conjunto con Bienestar Universitario y la Oficina de Admisiones y Registro Académico** deben asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y el Manual de Seguridad y Políticas de Informática en línea publicado en la web institucional www.uniatlantico.edu.co, SIG, Mapa de Procesos, Gestión Tecnológica y Comunicaciones, Manuales.

El estatuto estudiantil debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos inadecuados de información y TI que violen los términos y condiciones.

Usuarios Externos.
Todos los usuarios externos y personal de empresas externas deben estar autorizados por La Oficina de Informática, quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales. Los procedimientos para el registro de tales usuarios debe ser creado y mantenido por la Oficina de Informática en conjunto con la Oficina de Talento Humano. Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las credenciales de acceso al sistema (usuarios externos) cuales deben ser de perfiles específicos y tener caducidad no superior a ***la vigencia contractual***, renovables de acuerdo a la naturaleza del usuario.

6. SEGURIDAD INSTITUCIONAL

Toda persona que ingresa como usuario nuevo a la Universidad del Atlántico para utilizar equipos de cómputo y emplear servicios informáticos debe aceptar las condiciones de confidencialidad, del buen uso de los recursos tecnológicos y de información, así como cumplir los lineamientos y compromisos consignados en esta política y en el Manual de Seguridad y Políticas de Informática.

1.1 **Usuarios Nuevos.** Todo el personal nuevo de la Institución, deberá ser reportado por su jefe inmediato, interventor o supervisor del contrato al Departamento de Talento Humano quien es el ente facultado para reportar novedades y actualizaciones del personal (administrativo, contratistas, docentes tiempo completo/ocasional, monitores y otros) vinculado a la Universidad del Atlántico, debe reportar a la Oficina de Informática, para que asigne las herramientas y derechos correspondientes para el buen desarrollo de su objeto contractual (equipo de cómputo, recursos tecnológicos, cuentas de usuario y/o credenciales para acceder a los sistemas de información) o en el caso de cambio o retiro del cargo, revocar las credenciales de acceso al sistema.

1.2 **Capacitación en Seguridad de la Información y Manual de Funciones.** Todo servidor o funcionario nuevo en la Universidad del Atlántico deberá recibir inducción sobre sus funciones, Política y Estándares del SGSI y el **Manual de Seguridad y Políticas de Informática**, donde den a conocer los compromisos, responsabilidades, obligaciones para los usuarios y las sanciones que pueda incurrir en caso de incumplimiento.

7. PLAN DE IMPLEMENTACIÓN DEL MSPI

Basado en el diagrama presentado en el MSPI (Modelo de seguridad y privacidad de la información) publicado por el MINTIC, se elabora el plan de implementación que se muestra a continuación.

Gestión	Actividades	Tareas	Responsable
Activos de información	Definir formato para levantamiento de los activos de información de las dependencias	Creación de la metodología y del instrumento para el levantamiento de activos de información de los procesos de cada dependencia	Jefe de la Oficina de informática o un delegado
		Identificar y citar a los gestores de proceso de cada dependencia y realizar un acta	Jefe de la Oficina de informática o un delegado
	Realizar el levantamiento de los activos de información	Registro o actualización de los activos mediante el uso del formato creado en la actividad anterior, para su identificación y valoración	Jefe de cada dependencia o personas delegadas por los mismos
		Identificar o actualizar los activos de información de las dependencias.	Jefe de cada dependencia o personas delegadas por los mismos
		Compilar, validar y aceptar los activos de información para su publicación a cargo de cada líder de proceso (análisis cualitativo) (publicación y registro según ley 1712 de 2014)	Jefe de cada dependencia o personas delegadas por los mismos con el aval de la oficina jurídica y la oficina de informática
	Revisión de datos personales	Reportar al líder de la oficina de informática o al encargado de la seguridad de la información, los activos recolectados en el formato que correspondan a base de datos	Jefe de cada dependencia o personas delegadas por los mismos
	Publicación y registros de los activos de información según ley 1712 de 2014	Publicar los instrumentos de activos de la información consolidados (análisis cuantitativo)	

Gestión	Actividades	Tareas	Responsable
Gestión de riesgos	Revisión de lineamientos de riesgos	Revisar política y metodología, declaración de aplicabilidad de gestión de riesgos	Equipo de planificación de seguridad de la información
	Socialización	Socialización plan, Modelo de Seguridad y privacidad de la Información y plan de Continuidad de la operación	Jefe de la oficina de informática o un delegado

	Identificación de riesgos de seguridad y privacidad de la información	Convocar gestores de los procesos a reunión de análisis de riesgos y realizar el acta	Jefe de la oficina de informática o un delegado
		Identificación, análisis, aceptación, aprobación y evaluación de riesgos - seguridad y privacidad de la información y realizar plan de tratamiento, si aplica	Jefe de cada dependencia o personas delegadas por los mismos
	Seguimiento a la fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Jefe de cada dependencia o personas delegadas por los mismos
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Jefe de cada dependencia o personas delegadas por los mismos
	Plan de mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Jefe de cada dependencia o personas delegadas por los mismos
		Actualización guía gestión de Riesgos Seguridad de la información, de acuerdo a los cambios que sean solicitados	Equipo de planificación de seguridad de la información
	Monitoreo y revisión	Seguimiento de indicadores	Equipo de planificación de seguridad de la información

Gestión	Actividades	Tareas	Responsable
Gestión de incidentes de seguridad de la información	Seguimiento de incidentes de seguridad de la información	Seguimiento de incidentes de seguridad de la información	Jefe de cada dependencia o personas delegadas por los mismos
		Socializar incidentes	Jefe de cada dependencia o personas delegadas por los mismos
	Gestionar los incidentes de seguridad de la información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Jefe de cada dependencia o personas delegadas por los mismos
Acciones correctivas y oportunidades de mejora SGSI	Reporte del estado de las acciones correctivas y oportunidades de mejora	Seguimiento de las acciones correctivas y oportunidades de mejora	Jefe de cada dependencia o personas delegadas por los mismos
Planeación	Revisión de políticas de seguridad de la información	Actualizar Manual Políticas de Seguridad de la Información	Equipo de planificación de seguridad de la información
Gobierno digital	Gobierno digital	Actualizar el Plan de Seguridad y Privacidad de la Información.	Jefe de la oficina de informática o un delegado
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Equipo de planificación de seguridad de la información
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Equipo de planificación de seguridad de la información

8. REFERENCIAS BIBLIOGRAFICAS

- Guía emitida por el MINTIC.
- Modelo de seguridad y privacidad de la información v3.0.2.
- Norma ISO 27001:2013.
- Ley 1266 de 2008.
- Resolución 1581 de 2012 y decreto reglamentario 1377 de 2013.

9. CONTROL DE CAMBIOS

VER.	FECHA	ELABORÓ	REVISÓ Y APROBÓ	DESCRIPCIÓN
0	01/11/2020	Alvaro Castellar	Walberto Cantillo	VERSIÓN ORIGINAL