EMPRESA SOCIAL DEL ESTADO UNIVERSITARIA DEL ATLÁNTICO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección de Tecnologías de la Información y la Comunicación – TIC´S

2023

Calle 57 No. 23-100, Barranquilla, Col.
Email: gerencia@eseuniversitariadelatlantico.gov.co
Teléfono: (605) - 3319538 EXT 3100

TABLA DE CONTENIDO

Calle 57 No. 23-100, Barranquilla, Col.
Email: gerencia@eseuniversitariadelatlantico.gov.co
Teléfono: (605) - 3319538 EXT 3100

1. OBJETIVO:

Asegurar la adopción integral del Modelo se Seguridad y Privacidad de la Información (MSPI) bajo un enfoque de mejora continua que permita preservar la confidencialidad, integridad y disponibilidad de la información.

1.1 OBJETIVOS ESPECIFICOS

- Establecer un cronograma basado en el ciclo de mejora continua para la adopción integral del Modelo de Seguridad y Privacidad de la Información.
- Establecer medidas de implementación y de verificación de los controles previstos en el Modelo de Seguridad y Privacidad de la Información con base en los riesgos identificados de seguridad de la información en la E.S.E. Universitaria del Atlántico.

2. ALCANCE:

El plan está previsto para el alcance del sistema de gestión de seguridad de la información de la E.S.E. Universitaria del Atlántico UNA. Con el propósito de realizar una eficiente gestión de riesgos de Seguridad Digital en la E.S.E. Universitario del Atlántico, esta actividad se debe realizar integrando los procesos de la E.S.E. con este plan, mediante el uso de buenas prácticas y lineamientos nacionales, y locales, con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. A partir de lo anterior se definen los lineamientos mediante una guía para la gestión de riesgos de Seguridad Digital, para el tratamiento de los riesgos asociados a la información que es soportada por compontes tecnológicos en el entorno digital.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que superen el NRA (nivel de riesgo aceptable), de igual manera se deben monitorear los riesgos residuales periódicamente según la planeación de la entidad.

3. **MARCO LEGAL:**

• Constitución Política. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data; Artículo 20. Libertad de Información.

• Ley 527 de 1999. “Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”

• Ley 594 de 2000. “Ley General de Archivo”

• Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;”

• Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”

• Ley 1266 de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países

• Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. Art. 199. Espionaje; Art. 258. Utilización indebida de información; Art. 418.

Revelación de Secreto; Art. 419. Utilización de asunto sometido a secreto o reserva; Art. 420. Utilización indebida de información oficial; Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública; Artículo 463. Espionaje.

• Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.

• Ley 1437 de 2011. “Procedimiento Administrativo y aplicación de criterios de seguridad”.

• Ley 1480 de 2011. “Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas”.

• Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”.

• Decreto Ley 019 de 2012. “Racionalización de trámites a través de medios electrónicos criterio de seguridad”.

• Ley 1621 de 2013. “Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones”.

• Ley 1712 de 2014. “Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

• Decreto 1727 de 2009. “Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información”

Calle 57 No. 23-100, Barranquilla, Col.
Email: gerencia@eseuniversitariadelatlantico.gov.co
Teléfono: (605) - 3319538 EXT 3100

• Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”

• Decreto 2364 de 2012. “Firma electrónica”

• Decreto 2609 de 2012. “Expediente electrónico”

• Decreto 2693 de 2012. “Gobierno electrónico”

• Decreto 1377 de 2013. “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”

• Decreto 1510 de 2013. “Contratación pública electrónica”

• Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”

• Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 581 de 2012”

• Decreto 1078 de 2015, por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de Información y las Comunicaciones

• Decreto 1008 de 2018. “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector Tecnologías de la Información y las Comunicaciones”

• Decreto 1413 de 2017. “Por la cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2018, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

Calle 57 No. 23-100, Barranquilla, Col.
Email: gerencia@eseuniversitariadelatlantico.gov.co
Teléfono: (605) - 3319538 EXT 3100

• Decreto 415 de 2016. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2011 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones”

• Política Pública: CONPES 3701 de 2011 - Lineamientos de Política para Ciberseguridad y Ciberdefensa; CONPES 3854 de 2016 - Política Nacional de Seguridad digital; CONPES 3920 de 2018 – Política Nacional de explotación de Datos; CONPES 3975 de 2019 – Política Nacional para la transformación digital e Inteligencia Artificial.

• Resolución 1519 de 24 de agosto de 2020, por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

• Directiva 026 de 2020 – Diligenciamiento de la información en el índice de transparencia y acceso a la Información– ITA – de conformidad con las disposiciones del Art 23 de la 23 de la Ley 1712 de 2014.

4. RESPONSABLE: Dirección TIC´S

5. GLOSARIO:

- Activo: Todo aquello que representa valor para la organización [ISO 27000]
- Activo de información: Datos y conocimiento con valor para la organización [ISO 27000]
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701)

Calle 57 No. 23-100, Barranquilla, Col.
Email: gerencia@eseuniversitariadelatlantico.gov.co
Teléfono: (605) - 3319538 EXT 3100

- Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética (CONPES 3701).
- Cláusula: Capítulos principales de la norma (ej. ISO 27001)
- Conformidad: Cumplimiento de un requisito de orden técnico u organizacional.
  - Control: Políticas, procedimientos, lineamientos, dispositivos y en general todo aquello previsto para transformar un riesgo [ISO 31000].
  - Dominio: Categoría de seguridad de la información según se describe en el Anexo A de la ISO 27001 [ISO 27002]
  - Riesgo: De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias".
  - Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
  - Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información (ISO/IEC 27000).

5.1 ABREVIATURAS

SI: Seguridad de la información
GDA: Gestión Documental y Archivo
ITEP: Índice de Transparencia en Entidades Públicas
MSPI: Modelo de Seguridad y Privacidad de la Información
PROC: Procedimientos documentados
RRHH: Recursos humanos
SGSI: Sistema de Gestión de Seguridad de la Información.

6. GENERALIDADES

La E.S.E. Universitaria del Atlántico, buscando desarrollar el Modelo de Seguridad y Privacidad de la Información (MSPI) ha establecido una estrategia integral de aseguramiento de la información de forma tal que su adopción se está realizando de forma integrada con el Sistema de Gestión de Seguridad de la Información, considerando que la norma ISO/IEC 27001:2013 es base de ambos sistemas y que las guías técnicas desarrolladas por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, se basan en dicha norma y consideran el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia de Gobierno Digital: TIC para el Estado y TIC para la Sociedad.

A nivel metodológico, se ha seguido la estructura riesgo - control, de forma tal que las actividades iniciales están orientadas a conocer los riesgos de seguridad de la

información y como tratarlos, así como a asegurar la mejora continua en el proceso de gestión del riesgo y de seguridad de la información.

Las guías, dada su naturaleza de control, una vez alineadas con el Anexo A de la norma ISO/IEC 27001:2013 son aplicadas conforme a los resultados del análisis de riesgos:

Guía 1 - Metodología de pruebas de efectividad.
Guía 2 - Política General MSPI v1.
Guía 3 - Procedimiento de Seguridad de la Información.
Guía 4 - Roles y responsabilidades.
Guía 5 - Gestión Clasificación de Activos.
Guía 6 - Gestión Documental.
Guía 7 Gestión de Riesgos.
Guía 8 Controles de Seguridad de la Información.
Guía 9 Indicadores de Gestión de Seguridad de la Información.
Guía 10 Continuidad del Negocio.
Guía 11 Análisis de Impacto de Negocio.
Guía 12 - Seguridad en la Nube.
Guía 13 - Evidencia Digital.
Guía 21 - Gestión de Incidentes.

7. ACTIVIDADES

Las actividades para desarrollar en el Plan de Seguridad y Privacidad de la Información se describen a continuación:

7.1 Continuidad de la operación

Establecer metodologías, mecanismos y documentación que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.

7.2 Análisis de impacto de negocio

Establecer metodologías, mecanismos y documentación en el desarrollo del Análisis de Impacto de la E.S.E. Universitaria del Atlántico a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan sensiblemente la operación.

7.3 Seguridad en la Nube

Establecer metodologías, mecanismos y documentación para la gestión de la seguridad de la información alojada en la nube.

7.4 Análisis de vulnerabilidades.

Proceso de descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante.

7.5 Lineamientos y Documentación de Seguridad de la Información

Realizar los lineamientos y mantenimiento de la documentación relacionado con la seguridad de la información durante el desarrollo del modelo de seguridad y privacidad de la información.

7.6 Evaluación de Desempeño.

Realizar el seguimiento y evaluación de los indicadores de Seguridad de la información.

8. CRONOGRAMA:

ACTIVIDAD					
Continuidad de la operación.	Análisis de impacto de negocio.	Seguridad en la nube.	Análisis de vulnerabilidades	Lineamientos y Documentación de seguridad de la información.	Evaluación de desempeño.
DEFINICIÓN					
Establecer metodologías, mecanismos y documentación que responda a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas de la E.S.E. que se puedan ver comprometido por eventos naturales, o sean ocasionadas por el hombre.	Establecer metodologías, mecanismos y documentación en el desarrollo del análisis de impacto de la E.S.E. a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afecten sensiblemente la operación.	Establecer metodologías, mecanismos y documentación para la gestión de la seguridad de la información alojada en la nube.	Proceso de descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante.	Realizar los lineamientos y mantenimiento de la documentación relacionado con la seguridad de la información durante el desarrollo del modelo de seguridad y privacidad de la información.	Realizar el seguimiento y evaluación de los indicadores de Seguridad de la información.
2023					
FEBRERO MARZO ABRIL MAYO	ABRIL MAYO JUNIO JULIO	AGOSTO SEPTIEMBRE OCTUBRE NOVIEMBRE	SEPTIEMBRE OCTUBRE NOVIEMBRE	NOVIEMBRE DICIEMBRE	NOVIEMBRE DICIEMBRE

9. ANEXOS

El Modelo de Seguridad y Privacidad de la Información, el cual puede ser consultado (en su versión vigente) en línea y descargar las guías pertinentes, en la dirección: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

10. RECURSOS

La E.S.E. Universitaria del Atlántico en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La oficina de las Tics a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la E.S.E. en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo y el diseño de controles en Entidades Públicas – Riesgo de gestión, corrupción y seguridad digital. Herramientas para la gestión de riesgos (Matriz de Riesgos SGSI).
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos para los controles producto de la gestión de riesgos.