UNIVERSIDAD
NACIONAL
DE COLOMBIA

PROYECTO **CULTURAL, CIENTÍFICO Y COLECTIVO** DE NACIÓN

Sistemas Integrados

Sistema de Gestión de Seguridad de la Información - SGSI

Noviembre 2020
Dirección Nacional de Estrategia Digital - DNED

Universidad Nacional de Colombia
PROYECTO **CULTURAL, CIENTÍFICO Y COLECTIVO** DE NACIÓN

SGSI

El Sistema de Gestión de la Seguridad de la Información - SGSI hace parte del Sistema Integrado de Gestión Académica, Administrativa y Ambiental – SIGA a cargo de la Vicerrectoría General y está basado en un enfoque hacia los riesgos globales de un negocio.

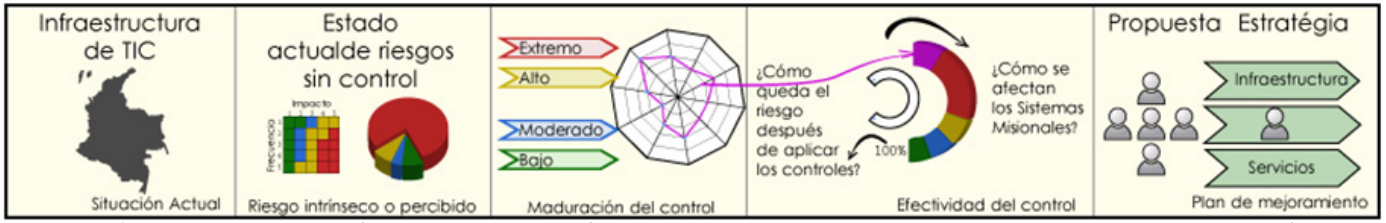
Tiene como finalidad establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

Normas a Integrar - SIGA

CONTEXTO DE SEGURIDAD

¿Cuáles son los Resultados del Estudio? (Fase-I)



¿Que **tenemos**?

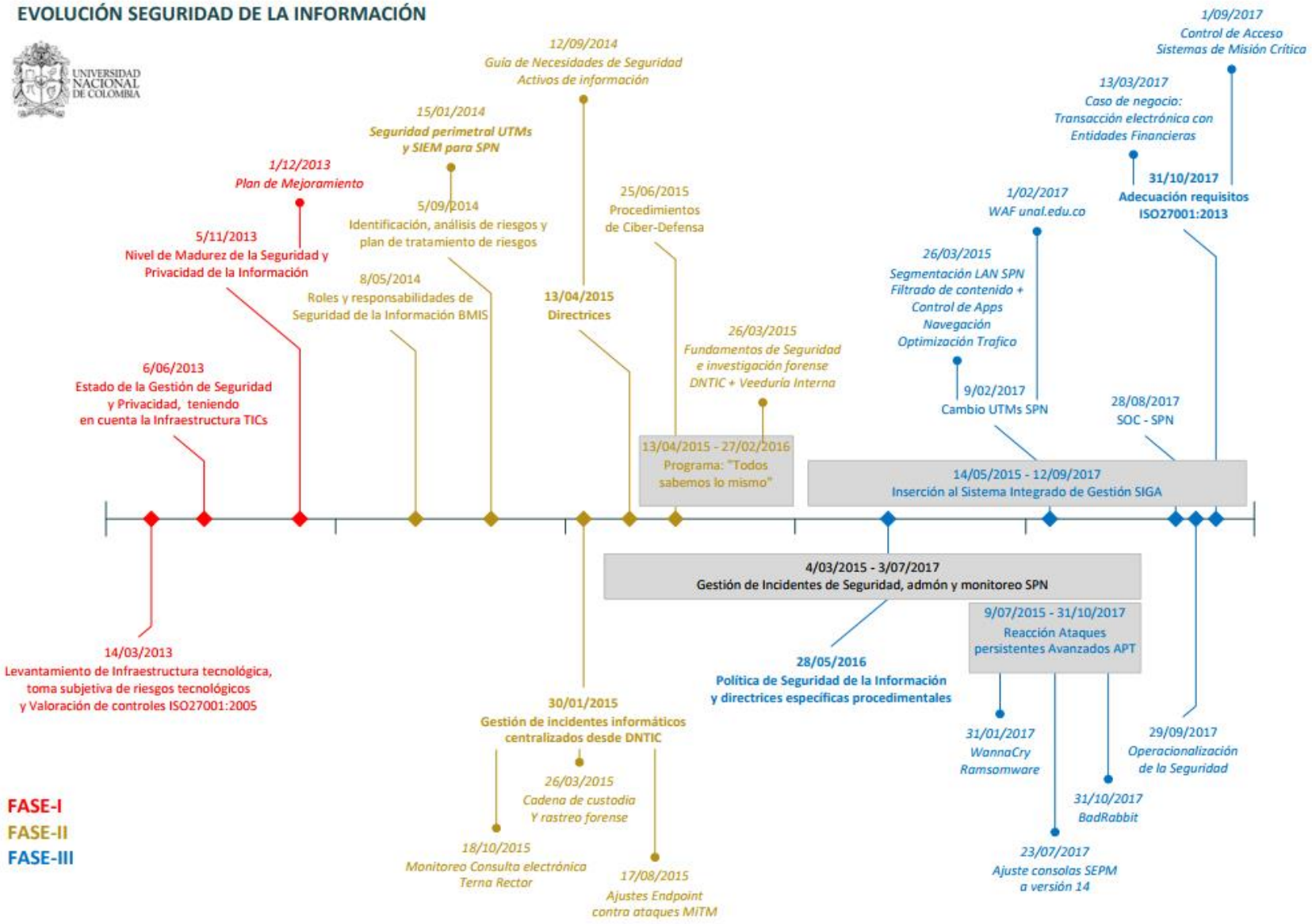
A qué estamos **expuestos**?

Cuán maduros son los **controles de TI**?

Ante un **ataque** o una **violación de seguridad**, somos capaces de: **Detectar**?, **Detener**?, Intervenir? **Mitigar**?, **Recuperar**? **Responder Legalmente?**

Que debemos **mejorar** para lograr las **condiciones mínimas** de **seguridad informática**?

EVOLUCIÓN SEGURIDAD DE LA INFORMACIÓN



FASES SGSI

Fase I – Levantamiento de la infraestructura tecnológica de seguridad y establecimiento del nivel de madurez de los controles en seguridad **(2013-2014)**

Se identificaron las principales brechas de seguridad existentes y se estableció el nivel de madurez de los controles en seguridad existentes.

Se ejecutaron actividades asociadas al levantamiento de la infraestructura tecnológica de seguridad informática utilizada por las Oficinas de Tecnología (OTIC) de las Sedes Bogotá, Medellín, Manizales, Palmira, Amazonía, Orinoquía y Caribe, incluyendo en el levantamiento las ubicaciones satélite de cada sede.

Logros: Diagramas de infraestructura, brechas de seguridad, plan de recomendaciones y mejora, lo que motivó el fortalecimiento de controles de perímetro.

FASES SGSI

Fase II – Establecimiento de los requisitos mínimos de un SGSI **(2015-2016)**

Con el fin de orientar las decisiones en materia de seguridad, se estiman los recursos necesarios y se define un cronograma para atender los riesgos que se identifiquen, en aras de establecer los requisitos mínimos de un SGSI para toda la Universidad, con aplicación específica a las Oficinas de Tecnología y Comunicaciones (OTIC) en cada una de las sedes a nivel nacional.

Logros: Política de seguridad, Sistema de riesgo tecnológico, Análisis de seguridad a activos de información, directivas procedimentales y normativas: Backup y recuperación, habeas data y protección datos personales, procedimientos de ciber-defensa.

FASES SGSI

Fase III – Adecuación de los requisitos exigibles por el estándar ISO 27001:2013 **(2017-2018)**

Adecuar y desarrollar los requisitos exigibles por la norma ISO 27001:2013 para dos casos de negocio orientados al fortalecimiento y mejora del SGSI de la Universidad.

Realización de auditorías al SGSI en cada una de las sedes de la Universidad mediante las cuales se determinó el grado de satisfacción con los requisitos de la norma.

Política General de Seguridad Informática y de la Información

Objetivos

a. Definir disposiciones de propósito general - Asegurar protección de información de la Universidad.

b. Apoyar y orientar a Directivas en Seguridad Informática- Requisitos del negocio y Normas aplicables

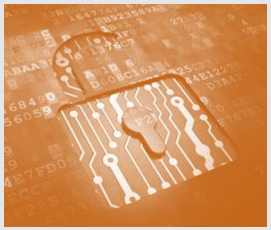
c. Proteger, preservar y administrar objetivamente la información de la Universidad, junto con las tecnologías informáticas utilizadas para su procesamiento frente a amenazas internas o externas - Asegurar cumplimiento de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

d. Mantener actualizada la Política de Seguridad Informática y de la Información- Vigente, operativa y auditada - Riesgos - Asegurar su permanencia y nivel de eficacia.

Política General de Seguridad Informática y de la Información

Responsables:

a. Dirección Nacional de Tecnologías de la Información y las Comunicaciones (DNTIC)
b. Oficinas de Tecnologías de la información y de las Comunicaciones (OTICs)
c. Comité Nacional de Informática y Comunicaciones (CNTIC)
d. Consejo Superior Universitario (CSU)
e. Dirección Nacional de Personal Académico y Administrativo
f. Dirección Jurídica Nacional
g. Gerencia Nacional Financiera y Administrativa
h. Áreas Usuarias



Política General de Seguridad Informática y de la Información

Reglas:

Se han establecido como necesarias 20 reglas que han sido orientadas al establecimiento, implementación, seguimiento, auditoría y promoción de la Política de Seguridad Informática.

Estas reglas deberán ser practicadas tanto a nivel de Gobierno en la DNTIC como en la Gestión por parte de las áreas de tecnología en cada Sede, Facultad, Centro o Instituto.

Dentro de las especificaciones de estas reglas se encuentran lo siguientes elementos:

1. Inventario de activos de información y recursos tecnológicos
2. Repositorio de arquitectura de seguridad informática
3. Indicadores (funciones / actividades / minimización de riesgos)
4. Estándares y lineamientos técnicos
5. Evaluación y seguimiento a la gestión de Seguridad
6. Sistemas de seguridad, contingencia y buen uso de los recursos
7. Directrices técnicas de aplicación institucional en materia de seguridad
8. Mecanismos para garantizar la integridad, confiabilidad, oportunidad, disponibilidad y seguridad
9. Manejo y mantenimiento de datos para consulta, ingreso, modificación, eliminación o divulgación

Política General de Seguridad Informática y de la Información

10. Responsabilidad de usuarios de la información contenida en sus equipos
11. Procesos y servicios (uso de activos informáticos en áreas claves de seguridad): Medidas técnicas, Recursos humanos / Capacidades, Legal y regulatorio y Educación / conciencia institucional y pública
12. Resultados de la Gestión del Riesgo (impacto positivo a nivel institucional)
13. Validación de la operacionalización de la seguridad (del acatamiento de políticas y disposiciones)
14. Disposiciones legales y reglamentarias en el ejercicio de la seguridad
15. Marco de cooperación científica y tecnológica
16. Actualización de las Políticas de seguridad a través de mecanismos del Sistema de Gestión de Calidad
17. Programas de Auditoría a la Seguridad informática y de la información
18. Procedimientos de seguridad de la información - cumplimiento de las políticas y estándares de seguridad

Acuerdo PSI - CSU

- El Comité Nacional de Tecnologías de la Información y las Comunicaciones - CNTIC en octubre de 2015 avala la propuesta de Política de Seguridad Informática y de la Información diseñada y elaborada por la Dirección Nacional de Tecnologías de la Información y las Comunicaciones (DNTIC).
- El Consejo Superior Universitario en mayo de 2016 aprueba la Política y emite el Acuerdo 228 que reza en su ***Artículo 2.*** *Incluir en el Sistema Integrado de Gestión Académica, Administrativa y Ambiental – SIGA y el Sistema de Control Interno, la Política de Seguridad Informática y de la Información de la Universidad Nacional de Colombia.*
- *Link:* **https://dntic.unal.edu.co/index.php/gobierno-tic-s/politicas**

Gestión de Riesgos y Certificación

Se plantea la necesidad de definir parámetros de evaluación del riesgo considerando aspectos de confidencialidad, integridad y disponibilidad, evaluados mediante una matriz en la que se define el riesgo tolerable o permitido para la seguridad de la información.

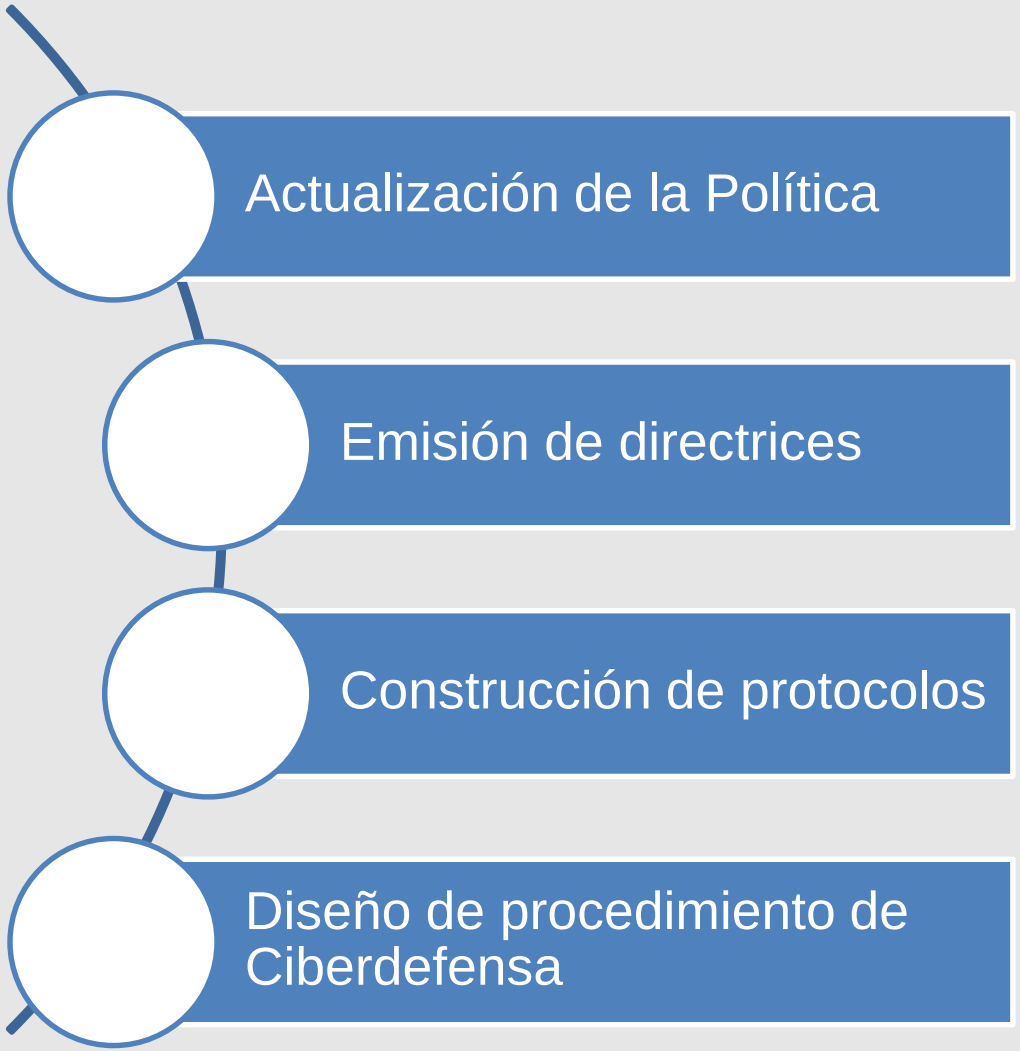
Teniendo en cuenta que se requiere un enfoque sistémico una de las metas de la Universidad es conseguir la certificación a través del estándar ISO 27001:2013 de por lo menos dos casos de negocio de seguridad informática y de la información.

Para el tema, se han definido los siguientes casos de negocio:

a. Control de Acceso

b. Transacción electrónica bancaria.

SGSI - Avanza en actividades



CUESTIONARIO

- ¿Sabe si existe una política de seguridad de la información (PSI) en la Universidad? ¿La ha leído? ¿Sabe dónde se encuentra publicada?
- *Si conoce la PSI* ¿Ha tenido la presunción de violación a las políticas de seguridad o cualquier situación que ponga en peligro la información institucional?
- ¿Ha identificado o sospecha de algún tipo de daño a la información o a la infraestructura de tecnología de la Universidad?
- ¿Sabe cómo actuar frente a la pérdida de información?
- ¿Sabe cómo alertar al respecto?

Gracias

Preguntas, comentarios y sugerencias