Política de Seguridad

Subcomisión de Ciberseguridad

Comisión de Conectividad y Sistemas

TEMARIO

- ¿Qué es una política de seguridad de la información?
- ¿Para qué sirve?
- ¿Por qué es necesaria una política de seguridad de la información en la Universidad?
- Gobernanza de la seguridad.
- Roles y funciones.
- Modelo del CIN.
- ¿Cómo empezar?
- Estado actual

¿Qué es una política de seguridad?

La política es:

- Un documento de alto nivel
  - Principios
  - directrices
- El pilar del Sistema de Gestión de Seguridad de la Información.
- Basada en leyes y estándares

La política debe:

- Ser aprobada a alto nivel
- Ser breve, sencilla y comprensible
- Ser comunicada
- Continuar con
  - otras políticas
  - Normativas
  - Procedimientos
  - guías

¿Para qué sirve la Política de Seguridad ?

Objetivo: Apoyo a la alta Dirección

Guia de Implementacion

¿Por qué es necesaria para las UUNN?

- En el pasado, la Seguridad estaba restringida a controlar la frontera de la Universidad defendiendo el interior del exterior.
- En la actualidad el escenario cambió completamente, y las fronteras son mucho más amplias.
- La seguridad no tiene un dueño.
- Los incidentes de seguridad aumentaron.
- La protección frente a incidentes de Seguridad, no es sólo un problema técnico.

¿Qué aporta a las UUNN?

- Organización de la concientización.
- Asignación de responsabilidades en lo que refiere a SI.
- Protección de los datos y la información que gestionan las UUNN.
- Protección de la infraestructura que da soporte a la información.
- Posibilidad de conocer y gestionar los riesgos en los activos.
- Posibilidad de minimizar la ocurrencia de incidentes de seguridad.
- Oportunidad para priorizar el gasto en TI.

Gobernanza de la seguridad

Niveles de la estructura de seguridad

Roles y Funciones - Comité de Seguridad

"Integrantes" del equipo de gobierno que garanticen que las políticas y estrategias en seguridad de la información están alineadas con las necesidades y estrategias de la institución.

Que tenga función y visión de gobierno, que transmita a la seguridad de la información cuál es la postura de la organización en materia de Seguridad de la Información.

- que establezca el Nivel de Seguridad requerido por los servicios
- que fije el balance entre seguridad y usabilidad
- que determine el Nivel de riesgos asumible
- que sepa y establezca hasta donde la organización quiere asumir un riesgo o no
- que revise la coherencia con la estrategia y políticas de la institución
- que coordine la comunicación

Roles y Funciones - Responsable de Seguridad

Persona con acceso directo a los niveles directivos de la organización (equipo de gobierno) que se responsabilice de que las directrices y políticas marcadas en materia de seguridad de la información se llevan a cabo de forma eficiente, algunas de estas tareas son:

- Supervisar y controlar del SGSI, no se hará cargo de implementar las medidas pero sí debería estar atento a que se hagan
- Revisar periódicamente los riesgos, porque hay nuevas regulaciones, o la organización cambió, o la institución tiene nuevos intereses o se modificaron sus procesos o servicios.
- Realizar propuestas en materia de seguridad de la información, proponer buenas prácticas en seguridad,
- Establecer contacto con CSIRTs de referencia que apoyen a la organización,
- Coordinar las acciones de formación y concienciación internas,

Roles y Funciones - Responsable de TI

Persona con acceso directo a los niveles directivos de la organización (equipo de gobierno) y capacidad de gestión de la operativa del Sistema, que implemente las medidas, instrucciones y procedimientos técnicos que se definan en el SGSI. En relación a la Seguridad algunas de sus tareas son:

- Desarrollar e implementar los controles definidos en la política, a nivel operacional: servidores, comunicación, sistema, etc.
- Elaborar y poner en práctica procedimientos e instrucciones para el personal técnico.

Modelo del CIN

- Basada en el modelo de la ONTI (año 2015).
  - Basado en la ISO 27002:2005
  - Modelo propuesto para las UUNN, tomando como referencia estándares nacionales e internacionales reconocidos, tales como las Normas IRAM-ISO/IEC 27001, 27002 y 20000-1.
  - Decisión Administrativa 641/2021 (Junio 2021), como marco institucional
- Estructura
  - Política
  - Guia de políticas complementarias
    - 14 dominios con propuestas de políticas

¿Cómo empezar?

- Definir el comité y darle entidad (haciéndolo aprobar por quien corresponda). Se recomienda que el comité sea de carácter más resolutivo que de debate.
- Designar al responsable de seguridad de la información.
- Hacer aprobar la política por el órgano de la UUNN que corresponda.

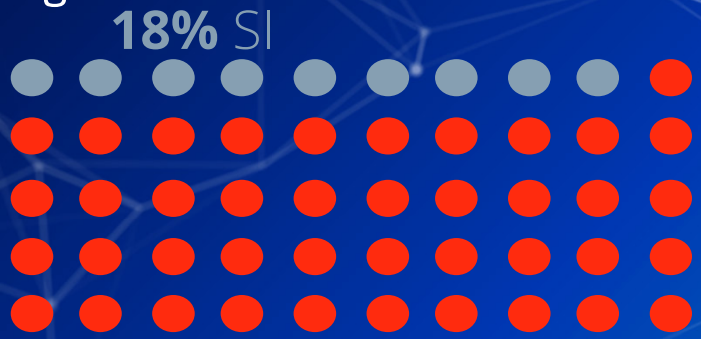
¿Cómo seguir?

Una vez definido el alcance de la política, es necesario identificar los activos de información, clasificar la información que procesan, almacenan o transfieren, finalizando el análisis de riesgos para determinar los pasos a seguir.

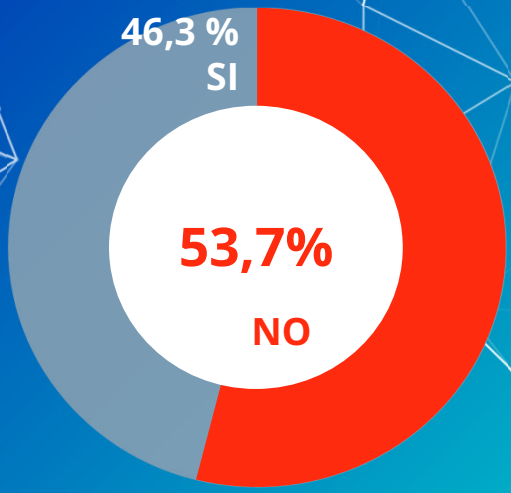
- Crear el árbol de activos de información, considerando dependencia entre ellos.
- Clasificar la información .
- Realizar el análisis de riesgos, esto ayudará a determinar el orden para comenzar a aplicar seguridad.
- Realizar análisis de vulnerabilidades de los activos.
- Revisar la guía, considerando los controles de seguridad.
- Realizar una lista de acciones a realizar en cada activo.

Informe situación de la gestión de la **Ciberseguridad en las UUNN**

¿Cuentan con área de seguridad informática?



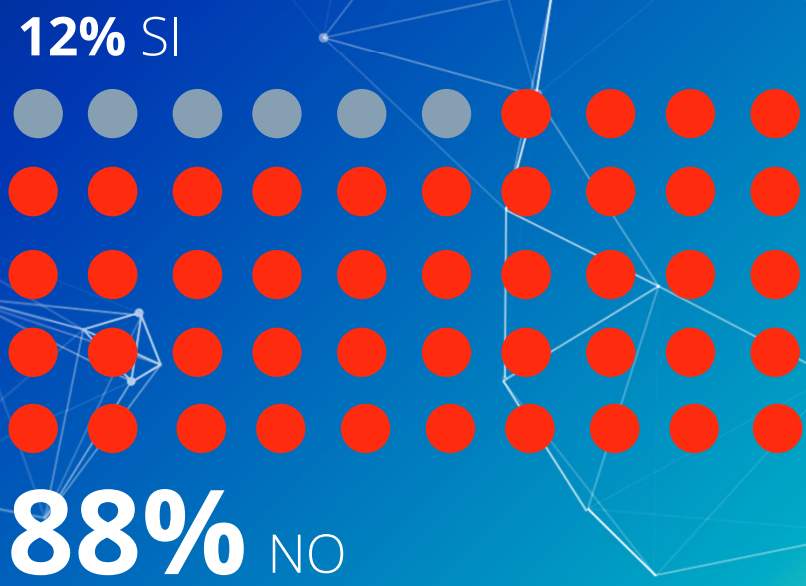
Sobre las que **NO tienen** área de seguridad, **¿está previsto tenerla en el corto plazo?**



Informe situación de la gestión de la **Ciberseguridad en las UUNN**

¿Cuentan con políticas de seguridad?

Sobre relevamiento de 55 UUNN



¿Cómo pueden ayudar?

MUCHAS GRACIAS

Preguntas?

Pueden encontrarnos en

- subcociberseg@campus.ungs.edu.ar
- https://www.cin.edu.ar