Política de Seguridad de la Información

Subcomisión de Ciberseguridad
Comisión de Conectividad y Sistemas
CIN

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?
- Espacio de preguntas

¿Qué es una Política de Seguridad? (PSI)

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 / plasmarse
  - Otras políticas.
  - Normativas.
  - Procedimientos.
  - Guías.

¿Para qué sirve la PSI ?

Objetivo: Apoyo a la alta Dirección

Guía de Implementación

¿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 dónde 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 PSI por el Órgano de la UUNN que corresponda.

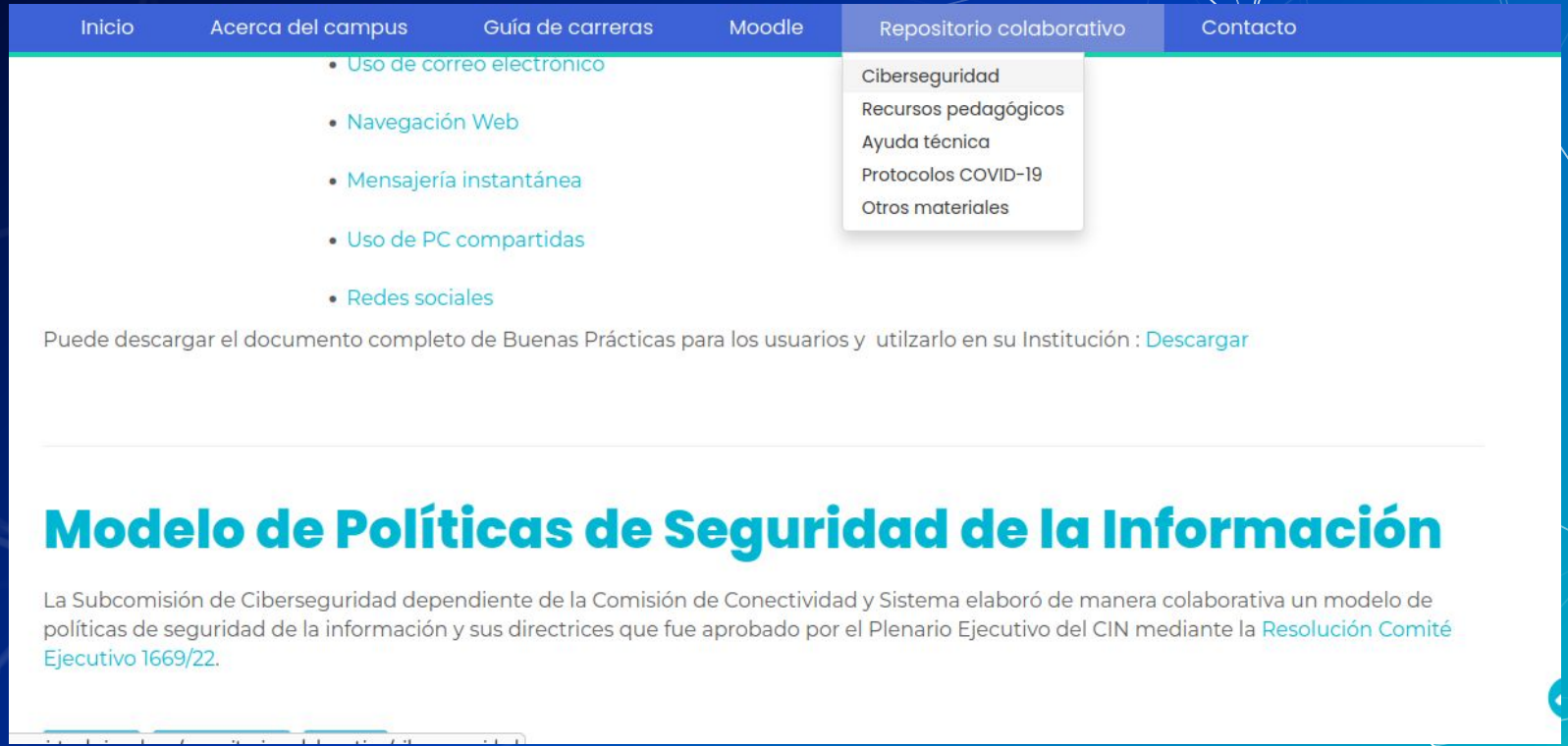
¿Cómo seguir?

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

- Crear el árbol de activos de información, considerando las dependencias entre ellos.
- Clasificar la información .
- Realizar el análisis de riesgos: Ayudará a determinar el orden para comenzar a implementar seguridad.
- Realizar el análisis de vulnerabilidades de los activos.
- Revisar la guía, considerando los controles de seguridad.
- Realizar una lista de acciones a llevar a cabo sobre activo.

¿Cómo ayudar?

https://campusvirtual.cin.edu.ar/
(https://campusvirtual.cin.edu.ar/files/1669-22.pdf)


Inicio
Acerca del campus
Guía de carreras
Moodle
Repositorio colaborativo
Contacto
Ciberseguridad
Recursos pedagógicos
Ayuda técnica
Protocolos COVID-19
Otros materiales
• Uso de correo electrónico
• Navegación Web
• Mensajería instantánea
• Uso de PC compartidas
• Redes sociales
Puede descargar el documento completo de Buenas Prácticas para los usuarios y utilzarlo en su Institución : Descargar
Modelo de Políticas de Seguridad de la Información
La Subcomisión de Ciberseguridad dependiente de la Comisión de Conectividad y Sistema elaboró de manera colaborativa un modelo de políticas de seguridad de la información y sus directrices que fue aprobado por el Plenario Ejecutivo del CIN mediante la Resolución Comité Ejecutivo 1669/22.

Guía de Buenas Prácticas en Ciberseguridad

El presente proceso de transformación digital que atraviesan nuestras Instituicones, convierten a la información en uno de los principales activos. Las buenas prácticas de ciberseguridad son una prioridad para mantener los datos de manera segura.

La Subcomisión de Ciberseguridad elaboró una Guía de Buenas Prácticas destinadas a los usuarios donde se recorren de manera sintética y precisa los principales aspectos a tener en cuenta.

En la guía se recorren los siguientes tópicos:

- Contraseñas
- Entorno de trabajo
- Uso de correo electrónico
- Navegación Web
- Mensajería instantánea
- Uso de PC compartidas
- Redes sociales

MUCHAS GRACIAS POR SU ATENCIÓN

Contacto:

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

Espacio de preguntas