UPAEP	Versión 2
	Política de Seguridad de la Información en el sistema UPAEP
Dirección General de Gestión y Finanzas **Dirección de Plataforma Tecnológica**	Elaborada por: Vicente Hernández Luna Fecha: febrero-2024
	Autorizada por: Comité de Seguridad de la Información Fecha:
	DOCUMENTO PÚBLICO

Introducción

La Dirección de Plataforma Tecnológica ha desarrollado la presente Política de Seguridad de la Información en el sistema UPAEP que establece la visión de la Institución en ese campo y tiene como objetivo general el de obtener el máximo beneficio de las tecnologías de información y comunicación (TIC's) en un entorno confiable y resiliente, con un enfoque preventivo y orientado a la gestión de riesgos, que se traduzca en beneficios para la institución y la comunidad universitaria de acuerdo con los valores, misión y visión del sistema UPAEP y garantizando los principios fundamentales de la ciberseguridad, que son:

- Disponibilidad: la información estará disponible y utilizable cuando sea requerido
- Confidencialidad: la información es vista o accedida solo por quien tiene los privilegios para ello
- Integridad: la información está completa, es confiable y protegida contra modificaciones no autorizadas
- Autenticidad: las transacciones y los elementos que intervienen en ellas son confiables
- No repudio: evitar que una entidad, órgano o persona que haya enviado o recibido información alegue ante terceros que no la envió o recibió

Para ello se reconocen:

A. La importancia de las tecnologías de información y comunicación (TIC's) en el funcionamiento de la institución
B. La existencia de una serie de riesgos asociados al uso de las TIC´s
C. La necesidad de una cultura de ciberseguridad

Principios rectores y objetivos

Los principios rectores de la presente Política son:

- Gestión de riesgos: Evaluación y gestión de los escenarios de riesgo en materia de Ciberseguridad por medio de enfoques preventivos y correctivos, con la intención de eliminar o minimizar el impacto de las amenazas y riesgos del ciberespacio.
- Cumplimiento de la legislación y normas que sean de aplicación.
- Colaboración multidisciplinaria: dado que la Seguridad de la Información es una tarea global de toda la institución es necesario promover la intervención de diferentes áreas.

Los objetivos estratégicos que persigue la presente política son:

- Garantizar la actividad del Sistema UPAEP: Fortalecer los mecanismos en materia de ciberseguridad para proteger la actividad de la institución garantizando la confianza y continuidad en la prestación de servicios y trámites a la comunidad universitaria favoreciendo el máximo aprovechamiento y uso responsable de los sistemas institucionales, infraestructura, equipos y accesorios de cómputo, licencias y cualquier otro componente de tecnología de la información y comunicación, así como la convivencia y el desarrollo de las actividades propias de cada uno de los integrantes del mismo.
- Proteger la información y los sistemas de acceso a ella para asegurar la integridad, confidencialidad y acceso necesario a la misma.
- Cumplir con la legislación referente a la protección de datos y cualquier normativa que sea de aplicación en el ámbito de la Seguridad de la Información, generando las condiciones para que la comunidad universitaria realice sus actividades de manera responsable, libre y confiable con el apoyo de las tecnologías de información, previendo e investigando conductas inadecuadas que puedan afectar a las personas, sus derechos e información, la institución y el correcto funcionamiento de la infraestructura de TI.

Alcance

La Seguridad de la Información se entiende como habilitador para el desarrollo de todo el potencial inherente a las TIC’s y como pieza clave para el progreso del sistema UPAEP, por lo tanto debe estar alineada a los objetivos institucionales y evolucionar conforme a las necesidades de la institución en lo referente la seguridad en las TIC’s y tener la capacidad de adaptación y mejora continua frente a los nuevos retos, riesgos, amenazas y vulnerabilidades futuras, en el corto, mediano y largo plazo.

Por todo ello el alcance de la presente Política en el sistema UPAEP es global y afecta a toda la comunidad en los siguientes aspectos:

- el uso correcto de sistemas institucionales.
- el uso correcto de infraestructura, equipos de cómputo, licencias y accesorios de cómputo.
- el uso correcto de la información a la que un usuario tenga acceso autorizado.

Referencias marco normativo

El marco normativo de referencia de la Política de Seguridad de la Información en el sistema UPAEP es:

- ISO/IEC 27001:2013: Sistema de Gestión de Seguridad de la Información
- ISO/IEC 27014:2020: Gobierno de Seguridad de la Información
- NIST Cybersecurity Framework v1.1:
- ITIL v3
- Ley Federal de Protección de Datos Personales en Posesión de Particulares y Reglamento que la desarrolla

Gestión de Riesgos

Principalmente el enfoque de esta Política es preventivo y orientado a la gestión de riesgos por lo tanto se requiere un ejercicio continuo en ese sentido.

Por lo tanto se establece la necesidad de realizar el Análisis de Gestión de Riesgos de forma periódica, mínimo una vez al año, y global, de acuerdo con la metodología o marco de referencia que se haya establecido.

Responsabilidades y Roles de la Seguridad de la Información.

La Seguridad de la Información recaerá sobre los siguientes responsables:

- Comité de Seguridad de la Información (CSI): cuya estructura, organización, funciones y responsabilidades se han establecido en el documento correspondiente.
- Responsable de Seguridad de la Información: sus responsabilidad serán:
    - Liderar la implantación del SGSI, gestionar la seguridad de la información de la institución de manera global, revisando periódicamente el estado de la misma y alineando la estrategia a los objetivos del sistema UPAEP.
    - Desarrollar y mantener el marco normativo de seguridad de la información y velar por su cumplimiento, estableciendo los controles y medidas técnicas y organizativas necesarias para asegurar los sistemas de información y llevando a cabo las acciones de comunicación necesarias.
    - Liderar las acciones integradas en el Plan de Concientización en Seguridad de la Información.

  - Elaborar el análisis de riesgos, identificando los procesos e información crítica y estableciendo las soluciones para mitigar las amenazas y la gestión de los riesgos.
  - Gestionar, notificar y analizar los incidentes de seguridad de la información realizando el seguimiento oportuno de acuerdo con el procedimiento establecido.
  - Definir indicadores en materia de seguridad de la información y llevar a cabo su revisión.
  - Controlar que las auditorías de seguridad se realicen con la frecuencia necesaria y revisar los informes de las mismas.
  - Reportar a las autoridades del sistema UPAEP, a la Dirección de Plataforma Tecnológica y al Comité de Seguridad de la Información las cuestiones relevantes en materia de seguridad de la información. Actuará como secretario del CSI.
- Equipo de Respuesta a Incidentes (IRT): su funcionamiento y responsabilidades será regulado de acuerdo con el Plan de Gestión de incidentes y estará formado por integrantes de diferentes áreas de la Universidad
- Dirección de Plataforma Tecnológica
- Dirección General de Gestión y Finanzas
- Secretaría General: como autoridad responsable del tratamiento de datos personales en el sistema UPAEP.

Marco normativo de Seguridad de la Información en el sistema UPAEP

A continuación se detallan las políticas, procedimientos y otros documentos que constituyen el marco normativo de seguridad de la información en la institución.

Estos documentos pueden ser públicos o de acceso restringido y estarán publicados en el Portal Institucional (PI) o en el Repositorio Interno de Políticas (RI), respectivamente.

El acceso a los documentos publicados en el Portal Institucional se hará desde la parte privada del mismo, previa autenticación del usuario.

Los documentos con visibilidad restringida se almacenarán en el Repositorio Interno de Políticas y solo serán accesibles desde esa ubicación y por lo usuarios a los que se les haya concedido ese permiso.

El desarrollo de todas las políticas se debe ajustar a la Guía de Elaboración de Políticas.

Documento	Acceso	Estado	RI	PI	Observaciones
Política de Seguridad de la Información en el sistema UPAEP	Público	Aprobada	✓	✓	El presente documento
Reglamento de uso de activos de TI	Público	Aprobado	✓	✓	
Estructura, Organización y Funciones del Comité de Seguridad de la Información	Público	Aprobada	✓	✓	
Guía de Elaboración de Políticas	Público	Aprobada	✓	✓	
Guía de Identificación de activos	Restringido	Aprobada	✓	×	
Metodología de Análisis y Gestión de riesgos de TI en UPAEP	Restringido	Aprobada	✓	×	
Política de Acceso Remoto	Público	Aprobada	✓	✓	
Política de Administración de Servidores	Restringido	Aprobada	✓	×	
Política de Identificación, clasificación y valoración de	Restringido	Aprobada	✓	×	Incluye el Inventario de activos de información y su clasificación.

Documento	Acceso	Estado	RI	PI	Observaciones
activos de información.					
Política de Respaldo y Plan de recuperación de desastres del Firewall	Restringido	Aprobada	✓	×	
Política de gestión de parches	Restringido	Pte. aprobar			
Política de gestión de vulnerabilidades	Restringido	Pte. aprobar			
Política general de contraseña de usuario	Público	Aprobada	✓	✓	
Políticas de Contraseñas de la Base de Datos	Restringido	Aprobada	✓	×	
Políticas de Acceso a la Base de Datos y Cambios en Unisoft	Restringido	Aprobada	✓	×	
Políticas de Contraseñas de usuario de UNISOFT	Público	Aprobada	✓	✓	
Políticas de Recertificación de permisos en UNISOFT	Restringido	Aprobada	✓	×	

Documento	Acceso	Estado	RI	PI	Observaciones
Guia elaboración Cuadro de Mando de Seguridad de la Información	Restringido	Aprobada	✓	×	
Plan de Concientización en Seguridad de la Información	Público	Aprobada	✓	✓	Se elaborará anualmente.
Política de Control de Accesos a Centros de Cómputo de UPAEP y zonas restringidas	Restringido	Pte. desarrollo	✓	×	
Política para la gestión de contraseñas de accesos privilegiados	Restringido	Aprobada	✓	×	
Política de incorporación de activos de TI de terceros a sistema UPAEP	Público	Aprobada	✓	✓	
Lineamientos sobre Seguridad de la Información en relaciones con proveedores y terceros.	Público	Pte. desarrollo	✓	×	
Política de retención de registros	Público	Pte. desarrollo	✓	×	

Documento	Acceso	Estado	RI	PI	Observaciones
Plan de Gestión de incidentes de Seguridad de la Información	Restringido	En desarrollo	✓	×	
Lineamientos y recomendaciones de uso de recursos de videoconferencia	Público	Aprobada	✓	✓	

Gestión de incidentes

Se llevará a cabo de acuerdo a lo dispuesto en el "Plan de Gestión de incidentes de seguridad de la información" que será el marco que garantice la adecuada comunicación y manejo sistemático de eventos e incidentes de seguridad, de modo que puedan ser resueltos de manera oportuna y permita la conservación de las pruebas que sean necesarias para la posterior investigación forense, así como la mejora de los procesos de evitar la recurrencia.

Sanciones en caso de incumplimiento

Cualquier violación e incumplimiento a lo previsto en esta política o en cualquiera de los documentos que componen el marco normativo de Seguridad de la Información en el sistema UPAEP será sancionado con:

1. Amonestación escrita
2. Suspensión temporal del servicio, herramienta, acceso o uso del activo de TI, en caso de persistir en la falta o no atender las indicaciones. En este caso se notificará también al superior inmediato en caso de tratarse de un colaborador, al Director Académico en caso de tratarse de un estudiante o al Departamento de Adquisiciones en caso de tratarse de un proveedor.

   En caso de persistir en la falta o no atender las indicaciones:

a. En el caso de Colaboradores no cumplir con las políticas expresadas en este documento: Remite a quien incumple a lo especificado en el Reglamento de Colaboradores UPAEP Capítulo I artículos 85 a 87.
b. En el caso de Estudiantes: De acuerdo con lo dispuesto en el artículo 13, Capítulo V del Reglamento General de Estudiantes y Usuarios de Servicios Académicos.
c. En el caso de Terceros: Lo que se establezca en el Contrato de Prestación de servicios o adquisición y Acuerdos de Confidencialidad que se haya establecido con el mismo.

3. Reparación del daño causado cuando se amerite.

Aprobación, entrada en vigor y mejora continua

La entrada en vigor de la presente política, una vez aprobada por el Comité de Seguridad de la Información, se llevará a cabo un día después de su publicación en el Portal Institucional.

La presente política debe ser revisada por lo menos una vez al año.

Control de versiones del documento

Fecha	Versión	Elaborado	Autorizado	Comentarios
mar-2022	1.0	Vicente Hernández Luna	Comité de Seguridad de la Información	Versión inicial
ene-2024	2.0	Vicente Hernández Luna		• Se incluye clasificación del documento • Eliminar referencia a Estrategia de seguridad de la información en UPAEP • Se incluye Política de incorporación de activos de TI de terceros a sistema UPAEP • Se incluye referencia a sistema UPAEP