BUSINESS INFORMATION & DIGITAL SERVICES AREA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

IESE Business School
University of Navarra

Tabla de contenidos

Control de versiones

VERSIÓN	FECHA	RESUMEN	EDITADO / APROBADO	NIVEL DE CONFIDENCIALIDAD
0	01/12/2023	Edición de la política de Seguridad de la información	IESE	PÚBLICO
0	12/12/2023	Aprobación	Comité de Ciberseguridad y privacidad	PÚBLICO

1. INTRODUCCIÓN

La **UNIVERSIDAD DE NAVARRA** desarrolla, además de la labor puramente educativa, una importante labor sanitaria y de formación de alumnos de postgrado. En este sentido, la Universidad de Navarra ha establecido su propia **Política General de Seguridad de la Información**, dando cobertura a la propia Universidad y las entidades asociadas.
IESE Business School (IESE), como centro perteneciente a Universidad de Navarra, a través del presente documento y siguiendo las directrices marcadas por la Universidad de Navarra establece su propia **Política de Seguridad de la Información**, alineada con la anterior y con sus propias características debido a su actividad diferenciada, considerando los riegos y amenazas específicos en materia de seguridad de la información.

2. OBJETIVO

La presente política tiene como objetivo mostrar el compromiso de la Dirección de IESE, representada por su Comité de Ciberseguridad y Privacidad, respecto a la seguridad de la información y la protección de activos de información necesarios para el desempeño de las funciones descritas en el alcance, permitiendo así la consecución de sus objetivos de negocio y estratégicos.

Este compromiso se materializa mediante la implantación y el mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) en conformidad con el estándar internacional ISO/IEC 27001.

La **Política de Seguridad de la Información** tiene el objetivo fundamental de garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a las incidencias que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve el IESE para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- Disponibilidad: propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- Integridad: propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- Confidencialidad: propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- Autenticidad: propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.

- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en IESE serán:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de disponibilidad y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

3. ALCANCE

La presente Política de Seguridad de la Información se aplicará a todas las áreas y departamentos que componen el IESE, a sus sistemas y activos de información:

- A todos los departamentos, tanto a sus directivos como a empleados.
- A todos los campus de la institución.
- A los partners (clientes y proveedores) así como cualquier otra organización que tenga acceso a la información o los sistemas de la institución.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.

4. DISTRIBUCIÓN

Aprobada por la Dirección de IESE, esta Política debe ser accesible a todas las personas y organismos afectados, mediante la publicación en web pública y en la intranet corporativa. De igual modo, la Política se encontrará accesible para cualquier parte interesada u órgano competente que lo solicite por vía formal.

Todo el personal de IESE, así como los colaboradores externos de la misma, serán responsables de cumplir con la presente Política de Seguridad de la Información.

5. MARCO NORMATIVO

El control de la normativa y legislación de aplicación de esta política de seguridad de la información que se incluye dentro del Sistema de Gestión de la Seguridad de la Información de IESE; disponible en la "*Normativa en Seguridad de la Información*".

6. COMPROMISO DE LA DIRECCIÓN

La Dirección de IESE se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI de la institución, así como a demostrar liderazgo y compromiso respecto a éste, a través de la constitución del Comité de Ciberseguridad y Privacidad que tendrá la responsabilidad de:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que éstos sean compatibles con la estrategia de IESE.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del SGSI en los procesos de la institución.
- Asegurar que los recursos necesarios para el SGSI estén disponibles.
- Facilitar la comunicación de la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI.
- Asegurar que el SGSI consigue los resultados previstos.
- Apoyar a las personas para contribuir a la eficacia del SGSI.
- Promover la evolución y mejora continua en materia de seguridad de la información.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.
- Supervisar los indicadores para evaluar el resultado/cumplimiento.
- Velar en la adopción de las medidas necesarias para cumplir con las recomendaciones e indicaciones formuladas por las autoridades supervisoras en el ejercicio de su función, así como hacer seguimiento de las regulaciones en materia de Seguridad y Privacidad.

- Asegurar el desarrollo de medidas de concienciación y planes de formación del personal relacionado con la seguridad de la información y en los tratamientos de datos personales.

7. FUNCIONES Y RESPONSABILIDADES

IESE ha establecido una estructura organizativa para el desarrollo de la presente política con las siguientes funciones y responsabilidades:

Comité de Seguridad y Privacidad (el "Comité"), facilitará los recursos necesarios para el funcionamiento y mejora del SGSI, asignar las responsabilidades en materia de seguridad de la información, aprobar la Política de Seguridad de la Información en los términos de la norma ISO 27001, así como promover y apoyar la implantación de las medidas técnicas y organizativas necesarias, incluyendo auditorías, para minimizar los riesgos potenciales a los que se encuentra expuesta la información y sus posibles consecuencias.

Comisión de Seguridad, se constituye como un órgano de apoyo al Comité de Ciberseguridad y Privacidad para llevar el día a día primero de la implantación del Sistema de Gestión de Seguridad de la Información y después coordinar a todas las áreas implicadas en la mejora continua y la gestión diaria, apoyando al Comité de manera técnica. Será función de esta Comisión de Seguridad, la revisión y aprobación de todo el cuerpo normativo que emana de la presente Política de Seguridad de la Información.

CIO (Chief Information Officer) y los **Responsables de los activos de información** (detallados en el Análisis de Riesgos del SGSI), definirán los requisitos de seguridad, identificando y priorizando la importancia de los distintos activos de modo que los procesos más importantes y/o sensibles reciban mayor protección, pero procurando al mismo tiempo el equilibrio en la seguridad IT en su conjunto; aprobar los niveles de riesgo residual que se obtengan mediante el proceso de evaluación de riesgos y aprobar los planes de tratamiento de riesgos necesarios para reducir los riesgos a un nivel aceptable.

CISO (Chief Information Security Officer), propondrá medidas e implantará las seleccionadas para mitigar los riesgos, así como supervisar la seguridad de los activos de información y de las medidas de aplicadas.

Responsable de IT Compliance, como responsable del SGSI procurará que esta Política de Seguridad de la Información y las políticas, procedimientos y notas técnicas que deriven de la misma, se mantengan actualizadas y en revisión permanente y sean comunicadas a las partes interesadas; supervisar su cumplimiento, asegurar el cumplimiento de las normativas y legislación aplicable;

velar por que se documenten adecuadamente las acciones realizadas y las incidencias que ocurran; sugerir mejoras de los procesos y procedimientos relacionados con el cumplimiento normativo en el ámbito IT.

Delegado de Protección de Datos (DPO) será el encargado de procurar que los datos personales se traten y se protejan conforme al Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y las recomendaciones de las Autoridades de Control competentes.

Todo el personal de IESE, así como los colaboradores externos de la misma, serán responsables de cumplir con la presente Política de Seguridad de la Información.

7.1. OBJETIVOS DE SEGURIDAD

Los objetivos de seguridad de la información se establecerán, buscando la mejora continua, en base a:

- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la institución y afecta a su desempeño en seguridad de la información.
- Cambios en las directrices en la materia por parte de Universidad de Navarra.
- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta los siguientes elementos:

- Lo que se va a hacer.
- Por qué se va a hacer.
- Los recursos necesarios.
- El responsable.
- Plazo de consecución.
- Indicadores para evaluar el resultado/cumplimiento.

7.2. IMPLANTACIÓN Y MEJORA DEL SGSI

El despliegue del SGSI de IESE se iniciará a partir del Análisis de Riesgos, que permitirá determinar el nivel de riesgo de seguridad de la información en que se encuentra la institución e identificar los controles de seguridad necesarios para el tratamiento del riesgo y llevarlo a un nivel aceptable, así como las oportunidades de mejora, considerando las cuestiones internas y externas y los requisitos de las partes interesadas antes indicados.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada, mediante procedimientos, normativas, instrucciones técnicas, manuales, etc., revisados y aprobados por la Comisión de Seguridad, junto con la supervisión del Delegado de Protección de Datos.

La presente Política de Seguridad de la Información se desarrolla aplicando los siguientes requisitos mínimos y que deben incluirse en la documentación que soporta el SGSI:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Se deberá comunicar la información documentada de los controles de seguridad al personal de la institución (empleados/staff y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del SGSI.

Se realizarán auditorías que revisen y verifiquen el cumplimiento del SGSI basados en la norma ISO/IEC 27001, por lo que, en caso necesario, el personal afectado por el alcance deberá colaborar en éstas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

7.3. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por la Dirección de IESE, y prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

7.4. CLASIFICACIÓN DE LA INFORMACIÓN

La información documentada será clasificada en: pública, interna y confidencial, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en el procedimiento de clasificación, etiquetado y protección de la información.

7.5. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será examinada en las revisiones del sistema por la Dirección, a través de la Comisión de Seguridad que propondrá su continuidad o cambios al Comité de Ciberseguridad y Privacidad, siempre que se produzcan cambios significativos y como mínimo, una vez al año.

- Revisiones periódicas sistemáticas: Deberán realizarse cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de dicha Política.
- Revisiones no planificadas: Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual o haya causado un impacto en la seguridad de la información de IESE.

La revisión de la Política de Seguridad de la Información deberá garantizar que ésta se encuentra alineada con la estrategia, la misión y visión de IESE en materia de seguridad de la información y que asegura el cumplimiento de los objetivos de control establecidos.

7.6. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- al menos una vez al año (mediante revisión y aprobación formal)
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad

- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, se establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

7.7. INSTRUMENTOS DE DESARROLLO

Se establece un marco normativo en materia de seguridad de la información estructurado por diferentes niveles de forma que los objetivos marcados por el presente documento tengan un desarrollo específico.
La política de seguridad de la información estructurará su marco normativo en los siguientes niveles:

- La presente Política de Seguridad de la Información que establece los requisitos y criterios de protección de carácter global.
- Las normas de seguridad que definen qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.
- Las propone el responsable del SGSI y aprueba el CISO. La Comisión de Seguridad se encarga de garantizar la correcta implementación.
- Los procedimientos de seguridad en los que describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.
- Su aprobación dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado.

Además, se podrán establecer guías con recomendaciones y buenas prácticas.

En la medida de lo posible, toda la documentación será gestionada según establece el procedimiento vigente de Control de documentos y registros en IESE, que tendrá como objetivo establecer los criterios para el control de la documentación y registros de seguridad utilizados en el Sistema de Gestión de la Seguridad de la Información.

7.8. OBLIGACIONES DEL PERSONAL

Todo el personal con responsabilidad en el uso, operación, o administración de sistemas de la información y las comunicaciones tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información.

La Política de Seguridad de la Información estará accesible para todo el personal que preste sus servicios en los órganos y entidades a que se refiere el punto relativo al 'Alcance'.

Con el objetivo de fomentar la 'Cultura de la seguridad', el Comité promoverá un programa de concienciación en seguridad dirigido al personal de la institución.

El incumplimiento de la Política de Seguridad de la Información y su normativa de desarrollo dará lugar al establecimiento de medidas preventivas y correctivas encaminadas a salvaguardar los sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

7.9. RELACIONES CON TERCEROS

Cuando IESE preste servicios o ceda información a terceras partes, se les hará partícipe de esta Política de Seguridad de la Información y de las normas e instrucciones derivadas.

Asimismo, cuando IESE utilice servicios de terceros o ceda información a terceros se les hará igualmente partícipe de esta Política de Seguridad de la Información y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información. Todos los partners (internos y externos) quedarán sujetos a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de detección y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en esta Política de Seguridad de la Información.

En concreto, los terceros deberán garantizar el cumplimiento de la política de seguridad de la información basadas en estándares auditables que permitan verificar el cumplimiento de estas políticas. Asimismo, se garantizará mediante auditoría o certificado de destrucción/borrado que el partner cancela y elimina los datos pertenecientes a IESE a la finalización del contrato.

Cuando algún aspecto de la Política de la Seguridad de la Información no pueda ser satisfecho por una tercera parte, se requerirá un informe del CISO que precise los riesgos en que se incurre y la forma de tratarlos.

8. APROBACIÓN DE LA POLÍTICA

La presente “Política de Seguridad de la Información” queda aprobada en acta con fechas 12 de diciembre del 2023 del Comité de Ciberseguridad y Privacidad.