UNIVERSIDAD POLITÉCNICA SALESIANA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO, ALCANCE Y USUARIOS

El propósito de esta Política de alto nivel es definir los objetivos, dirección, principios y reglas básicas para la gestión de la seguridad de la información en toda la Universidad Politécnica Salesiana (UPS).

Los usuarios de este documento son todos los empleados, personal administrativo, docentes y estudiantes de la Universidad Politécnica Salesiana, así como también terceros externos que se vinculen con la institución.

La presente Política se aplicará a:

a. Cualquier sistema que se ejecute en un computador o dispositivo que se encuentre conectado a las redes universitarias y a todos los sistemas de información suministrados por la Universidad Politécnica Salesiana.
b. Toda información procesada por la Universidad Politécnica Salesiana en virtud de sus actividades operativas, independientemente de que se procese electrónicamente o de forma física (en papel), cualquier comunicación enviada hacia o desde la UPS y cualquier información (datos) generados en sistemas externos a la red universitaria pero que sean utilizados por la UPS.
c. Todas las partes externas que prestan servicios a la Universidad Politécnica Salesiana en materia de instalaciones de procesamiento de información.
d. Principales activos de información, incluyendo las ubicaciones físicas en las que opera la Universidad Politécnica Salesiana.

2. DOCUMENTOS DE REFERENCIA PARA APLICACIÓN EFECTIVA DE LA POLÍTICA

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Plan de Seguridad de la Información de la Universidad Politécnica Salesiana
- Metodología de evaluación y tratamiento de riesgos de la UPS
- Declaración de aplicabilidad del Plan de Seguridad de la Información de la UPS
- Carta de navegación 2019-2023 de la Universidad Politécnica Salesiana
- Política de la Continuidad del Negocio de la UPS
- Política de Datos Personales de la UPS y clasificación de la información
- Procedimiento para gestión de incidentes de la UPS

3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

Autenticidad: Proceso para identificar un usuario o un dispositivo, esto con la finalidad de otorgarle privilegios.
No repudio: Pilar para garantizar la comunicación y autenticidad, remitente no puede negar el envío y el receptor no puede negar la recepción.
Confidencialidad: Característica de la información por la cual solo está disponible para personas o sistemas autorizados.
Integridad: Característica de la información que garantiza que es modificada por personas o sistemas autorizados y de una forma permitida.
Disponibilidad: Característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.
Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información.
Declaración de aplicabilidad: Documento obligatorio establecido por la norma ISO/IEC 27001:2013 que determina los controles que serán implementados y los que serán omitidos (justificando su omisión).

4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1 OBJETIVOS Y MEDICIÓN

Los objetivos generales para el Plan de Seguridad de la Información son: reducir el grado de vulnerabilidad de las Tecnologías de la Información y Comunicación de la UPS a un mínimo No repudio: pilar para el aseguramiento garantía de la comunicación y autenticidad, remitente no puede negar envío y que el receptor no puede negar recepción impacto para el año 2023 considerando los SLA firmados con los usuarios; además de mitigar el daño ocasionado por potenciales incidentes. Las metas están en línea con los objetivos estratégicos de la UPS.
El Secretario Técnico de Tecnologías de la Información es el responsable de revisar los objetivos generales del Plan de Seguridad de la Información y de establecer nuevos fines.
Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por el Rector, Vicerrectores, Secretarios y Directores Técnicos y son aprobados por el Secretario Técnico de Tecnologías de la Información en la Declaración de Aplicabilidad.
Todos los objetivos deben ser revisados al menos una vez al año.
La Universidad Politécnica Salesiana medirá el cumplimiento de todos los objetivos. El Secretario Técnico de Tecnologías de la Información es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos una vez al año y corresponde al Secretario Técnico de Tecnologías de la Información analizar y evaluar los resultados y los reportará al Comité Informático de la Universidad Politécnica Salesiana.

4.2 REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Esta Política y todo el Plan de Seguridad de la Información, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales.

4.3 CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

El proceso de escoger los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de Aplicabilidad.

Los controles seleccionados y aplicados buscarán cumplir los siguientes requerimientos:

4.3.1 Evaluación de Riesgo de la Información

4.3.1.1 El grado de control de la seguridad requerida depende de la sensibilidad y criticidad de la información. El primer paso para determinar el nivel adecuado de seguridad es un proceso de evaluación de riesgos, cuyo fin será identificar y clasificar la naturaleza de la información que la UPS posee, las consecuencias adversas de las brechas de seguridad y la probabilidad de que ocurran esas consecuencias.

4.3.1.2 Dada la naturaleza descentralizada de la estructura de la UPS, la evaluación del riesgo debe llevarse a cabo en primera instancia por sus diferentes departamentos y ésta debe ser coherente con los principios generales de esta Política.

4.3.1.3 La evaluación del riesgo debe identificar los activos de información del departamento, definir la propiedad de dichos activos, y clasificarlas en función de su sensibilidad y/o criticidad para el departamento o la UPS en su conjunto. En la evaluación de riesgos, los departamentos deben considerar el valor de los activos, las amenazas a ese activo y su vulnerabilidad.

4.3.1.4 Cuando sea práctico, los activos de información deben ser etiquetados y manejados de acuerdo con su criticidad y sensibilidad.

4.3.1.5 Se debe definir, documentar e implementar normas para el uso aceptable de los activos de información.

4.3.1.6 Las evaluaciones de riesgos de seguridad de información deben ser repetidos periódicamente como parte de la ejecución operacional normal y cuando se realicen cambios en la infraestructura, los sistemas informáticos y los procesos de la UPS.

4.3.2 Datos Personales

Todo lo referente a Datos Personales, estará contemplado en la "Política de Datos Personales de la UPS y clasificación de la información".

4.3.3 Protección de Sistemas de Información y Activos

4.3.3.1 Después de haber completado una evaluación de riesgo de sus activos de información, los departamentos deben elaborar sus lineamientos de seguridad que se enmarcarán en las Políticas establecidas en este documento, la determinación de controles y procedimientos adecuados. Los propietarios de la información deben tener constancia de que los controles reducen cualquier riesgo residual a un nivel aceptable.

4.3.3.2 La información confidencial debe ser manejada de acuerdo con los requisitos establecidos en el siguiente punto.

4.3.4 PROTECCIÓN DE INFORMACIÓN CONFIDENCIAL

El tratamiento de la Información Confidencial, estará contemplado en el documento "Política de Datos Personales de la UPS y clasificación de la información".

4.3.5 ACCESO REMOTO

4.3.5.1 Cuando se requiera de acceso remoto, éste debe ser controlado mediante una política de control de acceso definida y los controles deben ser estrictos manteniendo el principio del mínimo acceso necesario.

4.3.5.2 Todo acceso remoto debe ser controlado por protocolos de control de acceso seguro usando los niveles apropiados de encriptación y autentificación.

4.3.6 COPIA DE INFORMACIÓN

4.3.6.1 El número de copias realizadas de información confidencial, ya sea en dispositivos o medios portátiles o como copias físicas, deben ser las mínimas requeridas y cuando sea necesario, se debe llevar un registro de esa distribución. Cuando ya no sea necesaria la copia debe ser eliminada o, en el caso de copias físicas, deben ser destruidas.

4.3.6.2 Todas las copias deben ser físicamente seguras.

4.3.7 RETIRO DE INFORMACIÓN CONFIDENCIAL

4.3.7.1 Se debe definir políticas y procedimientos para el retiro o destrucción de información confidencial.

4.3.7.2 Documentos confidenciales deben ser triturados de forma segura luego de su retiro.

4.3.8 USO DE DISPOSITIVOS O MEDIOS PORTÁTILES

4.3.8.1 Se deben definir procedimientos para la administración de medios removibles con el fin de asegurar que ellos estén apropiadamente protegidos de accesos no autorizados.

4.3.8.2 El dueño de la información debe revisar los permisos sobre los activos de información a su cargo antes de que éstos sean llevados fuera de la UPS.

4.3.8.3 En el caso de datos personales, se recomienda que todos los dispositivos y medios portátiles deben ser encriptados cuando la pérdida de dicha información pueda causar daño o angustia a los individuos.

4.3.8.4 La frase de encriptación de un dispositivo no debe ser almacenada en el mismo dispositivo.

4.3.9 INTERCAMBIO DE INFORMACIÓN Y USO DEL CORREO ELECTRÓNICO

4.3.9.1 Se deben implementar controles para asegurar que los mensajes electrónicos son protegidos adecuadamente.

4.3.9.2 El correo electrónico debe ser apropiadamente protegido del uso y acceso no autorizado.

4.3.9.3 El correo electrónico solo debe ser utilizado para enviar información confidencial cuando el destinatario es de confianza, el dueño de la información ha dado su permiso y los controles adecuados se han adoptado.

4.3.9.4 Se debe proveer una guía para la administración de los riesgos asociados con el uso de correo electrónico.

4.3.10 CONTROLES CRIPTOGRÁFICOS

4.3.10.1 Se deben definir procedimientos para soportar el uso de técnicas criptográficas para asegurar que solo el personal autorizado pueda tener acceso a información confidencial.

4.3.10.2 Se debe definir una política de criptografía y administración de claves, y verificar su cumplimiento con el fin de asegurar que los datos están apropiadamente asegurados y que los requerimientos tanto internos como externos han sido cumplidos.

4.3.11 DISEÑO Y DESARROLLO DE SISTEMAS

4.3.11.1 Una evaluación de riesgos debe ser llevada a cabo como parte del diseño y desarrollo de cualquier sistema que sea utilizado para almacenar información confidencial. La evaluación de riesgos debe ser repetida periódicamente en todos los sistemas existentes.

4.3.12 RESPALDO DE INFORMACIÓN

4.3.12.1 Los dueños de la información deben asegurarse que los respaldos y los procedimientos de recuperación sean definidos. Las copias de respaldo de todo activo de información importante deben ser probadas regularmente de acuerdo a una apropiada política de respaldo.

4.3.13 ETIQUETADO DE PROTECCIÓN DE COPIAS FÍSICAS

4.3.13.1 Los documentos que contienen información confidencial deben ser etiquetados como "Confidencial" o con una designación adecuada dependiendo de la clasificación adoptada por el departamento.

4.3.14 ALMACENAMIENTO DE COPIAS FÍSICAS

a. Cuando sea práctico, los documentos con información confidencial deben ser almacenados en armarios o gavetas, cuando no sea necesario y la información sea almacenada en estanterías abiertas, el espacio físico debe ser cerrado cuando se abandone por un tiempo considerable.
b. Las llaves de los armarios o gavetas, no deben ser dejados a la vista cuando el espacio físico no esté ocupado.

4.3.15 TRASLADO DE INFORMACIÓN CONFIDENCIAL FUERA DE LAS INSTALACIONES

4.3.15.1 La información confidencial no debe ser llevada fuera de la UPS a menos que esta pueda ser retornada en el mismo día o almacenada de manera segura durante la noche.

4.3.16 TRANSMISIÓN DE INFORMACIÓN CONFIDENCIAL

a. Si documentos confidenciales son enviados por fax, el remitente debe asegurarse de utilizar el número correcto y el destinatario se encuentre cerca de la máquina de destino listo para tomar la información inmediatamente luego de ser impresa.
b. Si documentos confidenciales son enviados mediante correo externo, de preferencia debe ser enviado por correo certificado y el remitente debe asegurarse de que los documentos sean adecuadamente sellados.
c. Si documentos confidenciales son enviados mediante correo interno, los documentos deben ser marcados como "Confidencial" con el nombre del destinatario claramente escrito.

4.4 CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio está reglamentada en la Política de gestión de la continuidad del negocio.

4.5 RESPONSABILIDADES

Las responsabilidades para el Plan de Seguridad de la Información son las siguientes:

4.5.1 COMITÉ INFORMÁTICO DE LA UNIVERSIDAD POLITÉCNICA SALESIANA

El Comité Informático debe revisar el Plan de Seguridad de la Información al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar minutas de dichas reuniones. Los objetivos de las verificaciones por parte del Comité Informático son:

a. Establecer la conveniencia, adecuación y eficacia del Plan de Seguridad de la Información.
b. Asegurar que los usuarios sean conscientes de esta Política.
c. Supervisar el cumplimiento de la presente Política.
d. Revisar de forma periódica el presente documento, teniendo en cuenta los cambios pertinentes en legislación, políticas organizacionales y obligaciones contractuales.
e. Asegurar que existe una dirección clara y el apoyo necesario para las iniciativas de seguridad de la información.

4.5.2 SECRETARIO TÉCNICO DE TECNOLOGÍAS DE LA INFORMACIÓN

a. El Secretario Técnico de Tecnologías de la Información es el responsable de garantizar que el Plan de Seguridad de la Información sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
b. El Secretario Técnico de Tecnologías de la Información es el responsable de la coordinación operativa del Plan de Seguridad de la Información, como también de informar su desempeño.
c. El Secretario Técnico de Tecnologías de la Información es el encargado de definir aspectos sobre la seguridad de la información y comunicará a la parte interesada (tanto interna como externa) cuando el caso lo amerite.
d. El Secretario Técnico de Tecnologías de la Información es el responsable de adoptar e implementar el plan de capacitación y concienciación, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.

4.5.3 CONSEJO DE SEGURIDAD DE LA INFORMACIÓN

a. El Consejo de Seguridad de la Información posee la responsabilidad última sobre la seguridad de la información en la Universidad Politécnica Salesiana, siendo el Consejo responsable de asegurar que la UPS cumpla con los requisitos externos pertinentes, incluidos los de carácter legislativo, este Consejo será nombrado por el Rector o su delegado.

4.5.4 DIRECTORES DE DEPARTAMENTOS

a. Los directores de departamentos son responsables de la seguridad de la información dentro de su área de gestión, debiendo garantizar que cada departamento ha puesto en marcha una política local de seguridad de la información para satisfacer sus propias necesidades, en consonancia con los requisitos de esta Política.
b. Los directores de departamentos deben definir de forma clara las funciones y responsabilidades específicas vinculadas a la seguridad de la información dentro de su área de gestión.

c. El responsable del departamento debe aprobar la Política, garantizar que se aplique y revisarla con regularidad.

4.5.5 USUARIOS Y PARTES EXTERNAS

a. Los usuarios de la información de la Universidad Politécnica Salesiana serán conscientes de sus propias responsabilidades individuales para cumplir con la presente Política institucional y las políticas departamentales de seguridad de la información.
b. Acuerdos con terceros relacionados con el acceso, tratamiento, la comunicación o la gestión de la información de la Universidad, o los sistemas de información, deben cubrir todos los requisitos de seguridad pertinentes, y serán tratados en acuerdos contractuales.
c. Todos los incidentes o debilidades de seguridad deben ser informados al Secretario Técnico de Tecnologías de la Información.

4.5.6 OTROS

a. La Secretaría Técnica de Gestión de Talento Humano implementará programas de capacitación y concienciación de empleados sobre seguridad de la información.
b. La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.

4.6 COMUNICACIÓN DE LA POLÍTICA

El Secretario Técnico de Tecnologías de la Información debe asegurarse de que todos los empleados, docentes y estudiantes de la Universidad Politécnica Salesiana, como también los participantes externos correspondientes, estén familiarizados con esta Política.

5. APOYO PARA LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

A través del presente documento, el Consejo Superior de la Universidad Politécnica Salesiana respalda la implementación y mejora continua del Plan de Seguridad de la Información y se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

5.1 COMPROMISOS

5.1.1 La Universidad Politécnica Salesiana reconoce el papel de la seguridad de la información para garantizar que los usuarios tengan acceso a la información que necesitan para llevar a cabo su trabajo. Los sistemas informáticos y los sistemas de información sustentan todas las actividades de la Universidad Politécnica Salesiana y son esenciales para sus funciones administrativas, actividades de investigación y docencia.

5.1.2 Cualquier reducción en la confidencialidad, integridad o disponibilidad de la información podría impedir que la Universidad Politécnica Salesiana funcione con eficacia y eficiencia. Además, la pérdida o la divulgación no autorizada de la información tiene el potencial de perjudicar el prestigio de la Universidad y causar pérdidas económicas.

5.1.3 Para mitigar estos riesgos, la seguridad de la información debe ser una parte integral de la gestión de la información, ya sea que se lleve a cabo en forma electrónica, en físico o en cualquier otro medio.

5.1.4 La Universidad Politécnica Salesiana se compromete a proteger la seguridad de su información y los sistemas de información con el fin de garantizar que:

a. La integridad de la información es conservada con el fin de que sea precisa, actualizada y que cumpla un propósito.
b. La información se encuentre siempre disponible para aquellos que la necesiten y no se presenten interrupciones en las actividades de la UPS.
c. La confidencialidad se mantenga en todo momento en la gestión de información.
d. La Universidad Politécnica Salesiana cumpla con los requisitos de seguridad tanto internos como externos.
e. El nombre de la Universidad Politécnica Salesiana sea salvaguardado.

5.1.5 Para cumplir estos propósitos, la Universidad Politécnica Salesiana está comprometida a implementar controles de seguridad que se ajusten a las mejores prácticas, tal como se establece en la norma ISO / IEC 27002:2013 Técnicas de Seguridad de la Información - Código de buenas prácticas para la gestión de seguridad de la información.

5.1.6 Las evaluaciones de riesgos de seguridad de la información deben realizarse para todos los sistemas de información sobre una base regular con el fin de identificar los principales riesgos de la información y determinar los controles necesarios para mantener los riesgos dentro de límites aceptables.

5.1.7 La Universidad Politécnica Salesiana se compromete a proporcionar educación y formación suficiente a los usuarios para asegurar que entienden la importancia de la seguridad de la información y, en particular, el ejercicio de atención adecuada al manejar la información confidencial.

5.1.8 El asesoramiento de especialistas en seguridad de la información se pondrá a disposición de toda la UPS.

5.1.9 Un grupo de seguridad de información, integrado por representantes de todas las partes pertinentes de la Universidad, asesorarán sobre las mejores prácticas y coordinarán la aplicación de los controles de seguridad de la información.

5.1.10 La Universidad Politécnica Salesiana establecerá y mantendrá los contactos pertinentes con otras organizaciones, autoridades policiales, los organismos reguladores y los operadores de redes y de telecomunicaciones en favor de su política de seguridad de información.

5.1.11 Las infracciones de seguridad de la información deben registrarse y notificarse a los órganos competentes de la UPS, que tomará las medidas e informará a las autoridades pertinentes.

5.1.12 Este resto de los documentos de apoyo a la presente Política se comunicarán, según sea necesario, a lo largo de toda la Universidad para cumplir con sus objetivos y necesidades.

6. CUMPLIMIENTO

6.1.1 Debe existir una política escrita definida de forma local para el manejo de información confidencial, ya sea electrónica o impresa, y una copia de los procedimientos debe ser proveída para todo usuario para que se encuentre consciente de sus responsabilidades.

6.1.2 Cualquier fallo en el cumplimiento de esta Política puede resultar en procesos disciplinarios.

6.1.3 Cualquier pérdida o divulgación no autorizada debe ser reportada al dueño de la información.

6.1.4 Los incidentes de seguridad de la información que involucren pérdida o divulgación no autorizada de información confidencial almacenada de forma electrónica deben ser reportadas a un Equipo de Respuesta de Emergencia para su posterior investigación.

6.1.5 Si la pérdida o divulgación no autorizada involucra datos personales, ya sea de forma electrónica o impresa, el Secretario Técnico de Tecnologías de la Información debe ser informado, ya sea mediante correo electrónico o vía telefónica.

7. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento está vigente válido desde el 01 de enero del 2015.

El responsable de este documento es el Secretario Técnico de Tecnologías de la Información, que debe verificar, y de ser del caso actualizarlo por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Número de empleados y participantes externos que cumplen una función en el Plan de Seguridad de la Información pero que no están familiarizados con el presente documento.
- Incumplimiento del Plan de Seguridad de la Información con las leyes y normas, las obligaciones contractuales y los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del Plan de Seguridad de la Información.

- Responsabilidades ambiguas para la implementación del Plan de Seguridad de la Información.

8. DISPOSICIÓN TRANSITORIA

Para garantizar la eficiente aplicación de esta Política, la UPS por medio de las instancias responsables se actualizará de acuerdo a los estándares nacionales e internacionales y mejores prácticas de TICs los siguientes documentos:

- Plan de Seguridad de la Información de la Universidad Politécnica Salesiana
- Metodología de evaluación y tratamiento de riesgos de la UPS
- Declaración de aplicabilidad del Plan de Seguridad de la Información de la UPS
- Política de la Continuidad del Negocio de la UPS
- Política de Datos Personales de la UPS
- Procedimiento para gestión de incidentes de la UPS.

Dado en la ciudad de Cuenca, a los 23 días del mes de marzo de 2022.

P. Juan Cárdenas Tapia, sdb. Ph.D.
RECTOR

Ana María Reino Molina
SECRETARIA GENERAL

CERTIFICO:

Que, el presente documento "Política de Seguridad de la Información" de la Universidad Politécnica Salesiana" fue aprobado por el Consejo Superior con Resolución N°210-11-2014-12-17 de fecha 17 de diciembre de 2014; y reformada con Resolución N°076-03-2022-03-23 de fecha 23 de marzo de 2022.

Ana María Reino Molina
SECRETARIA GENERAL

UNIVERSIDAD POLITECNICA SALESIANA
SECRETARIA GENERAL