UNIVERSIDAD DE LA SALLE

CONSEJO SUPERIOR
Acuerdo No. 036 de 2024
(1° de noviembre)

Por el cual se actualiza la Política de Seguridad de la Información de la Universidad de La Salle

EL CONSEJO SUPERIOR
DE LA UNIVERSIDAD DE LA SALLE
En ejercicio de sus funciones estatutarias y,

CONSIDERANDO

Que el Consejo Superior de la Universidad de La Salle, mediante el Acuerdo No. 017 del 5 de diciembre de 2019, actualizó la Política de Seguridad de la Información de la Universidad y por recomendación del Comité CIGIL, se presentó ante el Consejo de Coordinación en sesión del 29 de octubre, la propuesta de renovación de dicha política acorde con las buenas prácticas en la materia, y para armonizar sus disposiciones con lo referente al tratamiento de información, gestión documental y demás procedimientos que se incorporen en el Sistema Integrado de Gestión y Aseguramiento de la Calidad, y dicha instancia la consideró viable y decidió presentarla al Consejo Superior para su consideración y determinación.

Que de conformidad con lo dispuesto en el literal d. del artículo 23, del Estatuto Orgánico, corresponde al Consejo Superior, trazar las políticas académicas, de investigación, de extensión, de promoción y desarrollo humano, administrativas y financieras de la Universidad.

Que, en virtud de lo anterior,

ACUERDA

Artículo 1°. Actualizar la Política de Seguridad de la Información de la Universidad de La Salle, que tiene por objeto la protección de los activos de información, en términos de integridad, confidencialidad, disponibilidad y autenticidad para la gestión de los procesos académico-administrativos y para la toma de decisiones, la cual está contenida en los siguientes Artículos:

Artículo 2°. Declaración de la Política General de Seguridad de la Información

La Universidad de La Salle, se encuentra comprometida con el adecuado manejo y uso de sus activos de información y gestión del riesgo, mediante la adopción e implementación de la política de seguridad de la información, procedimientos e instrumentos, para salvaguardar los activos de información, para promover la prestación de servicios oportunos y seguros, en beneficio de todos los grupos de interés.

Artículo 3°. Ámbito de Aplicación.

La presente Política de Seguridad de la Información, y demás lineamientos que hacen parte de esta, aplica a toda la Comunidad Universitaria Lasallista y a los demás grupos de interés.

Artículo 4°. Definiciones

1. **Activos de información:** Es todo aquello que tiene un valor para la Universidad, cuya pérdida de integridad, confidencialidad, disponibilidad y autenticidad, podría generar un impacto no esperado. Los activos de Información, se clasifican en:

    a. **Información:** Es el conjunto de datos procesados, ordenados, estructurados y no estructurados, cuya consecución, almacenamiento o procesamiento requiere recursos físicos, económicos, tecnológicos y humanos;
    b. **Software:** Aplicaciones informáticas utilizadas en las actividades propias de cada proceso;
    c. **Hardware:** Elementos físicos y de infraestructura de tipo tecnológico que soportan servicios y procesos de Tecnologías de Información;
    d. **Redes:** Elementos de infraestructura de telecomunicaciones;
    e. **Persona:** Recurso humano involucrado en los procesos;
    f. **Gestión del Conocimiento:** Acciones que permiten potencializar la capacidad de la persona para que, a través de su experiencia y lecciones aprendidas, transfiera el

conocimiento adquirido para que la información mantenga su valor y se cumplan las metas y objetivos de la universidad.

g. **Procesos:** Conjunto secuencial de acciones ejecutadas para cumplir con los objetivos y la misión de la Universidad;
h. **Recursos Físicos:** Instalaciones y componentes físicos no tecnológicos.

2. **Administrador de Aplicación:** Se refiere a aquellos roles, cargos o personas que se encargan de la administración de una aplicación.
3. **Administrador de Base de Datos:** Se refiere a aquellos roles, cargos o personas que se encargan de administrar las bases de datos institucionales.
4. **Amenaza:** Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.
5. **Analítica de Datos:** Combinación de tecnología, herramientas y procesos que permiten transformar los datos almacenados en información, esta información en conocimiento y este conocimiento en decisiones para responder a un plan o una estrategia de la organización.
6. **Análisis de Riesgos:** Uso sistemático y metodológico para identificar, medir, estimar y evaluar riesgos sobre los activos de la información y detectar sus fuentes.
7. **Autenticidad de la Información:** Es la propiedad o atributo de la información que hace referencia a que el origen de esta es determinable y que su integridad no ha sido alterada.
8. **Bodega de datos:** Colección de datos totalizados y detallados históricamente orientados al sujeto, integrados, variantes en el tiempo y no-volátiles usados para soportar los procesos de toma de decisiones estratégicas para la organización.
9. **Ciclo PHVA –** El ciclo PHVA involucra o implica cuatro (4) etapas: (P) planear, (H) hacer, (V) verificar y (A) actuar. El proceso se realiza de manera lineal y la finalización de un ciclo precede el inicio del siguiente, por tanto, se vuelve cíclico.
10. **Cifrar / Descifrar:** Procedimiento utilizado para transformar una información en otra incomprensible, mediante la utilización de un algoritmo de cifrado y una clave o contraseña. La información inicial debe poderse recuperar a partir de la información incomprensible con una clave o contraseña, proceso que se denomina descifrar.
11. **Comunidad Universitaria Lasallista:** Grupo de personas conformado por los profesores, empleados administrativos, estudiantes y egresados de la Universidad de La Salle.
12. **Confidencialidad:** Es la propiedad o atributo de la información que hace referencia a que la información debe ser conocida y divulgada, únicamente por las personas, procesos o sistemas autorizados para tal fin.
13. **Continuidad de la misión institucional:** Plan estructurado que tiene como fin asegurar la continuidad de la operación de los procesos en el caso de una eventualidad o imprevisto que las afecte, impacte la continuidad de la operación.
14. **Control:** Medida o acción que modifica un riesgo para prevenir su materialización. Son las acciones, actividades, procesos o precauciones encaminadas a mitigar, reducir o eliminar un posible riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, ya sean de carácter administrativo, técnico o legal.
15. **Control Criptográfico:** Son los algoritmos de cifrados diseñados para confidencialidad, autenticidad e integridad de la información.
16. **Disponibilidad:** Característica que indica que la información sea accesible y utilizable por solicitud de personas, organizaciones, sistemas o procesos autorizados y de una forma permitida cuando sea necesario.
17. **Gobierno de seguridad de la información:** Sistema por el cual las actividades de seguridad de la información de la Universidad son dirigidas y controladas.
18. **Incidente de seguridad:** Se define como un evento que atenta contra la confidencialidad, integridad, disponibilidad y autenticidad de la información y los recursos tecnológicos de la Universidad. Cualquier intento de intrusión de la seguridad física y lógica de los sistemas, que puede producir fallas o interrupción en los procesos institucionales.
19. **Gestión de incidentes de seguridad de la información:** Proceso que permite detectar, alertar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
20. **Gestión de riesgos:** Proceso sistemático para administrar y controlar dentro de la Universidad los posibles riesgos a los que está expuesta en el desarrollo de su operación. Involucra la definición, identificación, evaluación o medición y el tratamiento de estos lo cual permite mitigar, transferir, aceptar o reducir su impacto.
21. **Impacto:** Es el costo para la Universidad a causa de la afectación por un incidente independiente de su tamaño o escala -, que puede o no ser medido financieramente, operacionalmente, afectación legal, o pérdida de reputación.
22. **Información institucional:** Es el conjunto de datos, estructurados y no estructurados que son insumos y/o resultados de cada uno de los procesos, servicios, procedimientos y actividades ejecutadas en la Universidad de La Salle.

23. **Información institucional sensible:** Es el conjunto de datos relacionados con los profesores, estudiantes, administrativos, egresados, usuarios, procesos, servicios e investigaciones cuyo conocimiento pueda poner en riesgo los intereses de los Titulares de la Información o los propios de la Universidad y su continuidad.
24. **Integridad:** Es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
25. **Inventario de Activos de información:** Listado de activos de información clasificados de acuerdo con su nivel de importancia, confidencialidad y valor para la Universidad.
26. **Líder de Proceso:** Se refiere a aquellos roles, cargos o personas que definen y gestionan cada una de las instancias de un proceso.
27. **Líder de Servicio:** Se refiere a aquellos roles, cargos o personas que se encargan de la toma de decisiones en cuanto al diseño y soporte de un servicio.
28. **Nivel de riesgo:** Evaluación del riesgo identificando su posible materialización frente al impacto y probabilidad de ocurrencia.
29. **Probabilidad:** Posibilidad que el riesgo se pueda materializar frente a un incidente de seguridad de la información.
30. **Proceso:** Conjunto de actividades interrelacionadas que, partiendo de unas entradas, las transforman y generan unas salidas.
31. **Recursos de tecnología:** Se refiere a todos los equipos de cómputo, dispositivos móviles, servidores, impresoras, scanner y software dispuestos por la Universidad para la recolección, generación, almacenamiento, trasferencia y usos de la información.
32. **Riesgo:** Es la exposición a una situación o amenaza determinada que puede suscitar una vulnerabilidad para causar o generar una pérdida o daño sobre un activo de información.
33. **Riesgo residual:** Es el riesgo que queda después de aplicar los controles al riesgo identificado.
34. **Seguridad de la Información:** Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad, disponibilidad y autenticidad de los activos de información de la organización.
35. **Seguridad informática:** Componente de seguridad de la información, referente a la implementación de medidas técnicas y establecimiento de controles a nivel de hardware, software y de recursos tecnológicos.
36. **Sistema de Información Integrado Lasallista -SIIL:** Es el conjunto de sistemas de Información articulados que facilitan la gestión de los procesos académicos y administrativos de la Universidad de La Salle.
37. **Terceros relacionados:** Se refiere a personas o instituciones que tienen relaciones contractuales o de otro tipo con la Universidad y que no son empleados, profesores, estudiantes o egresados.

Artículo 5°. De la Clasificación de los Activos de Información

Para los efectos de la presente política la Universidad define los siguientes niveles de clasificación para los activos de información:

1. **Nivel 1: Confidencial.** Información con nivel alto de confidencialidad que por normas legales estatutarias y reglamentarias la Universidad determine tal carácter. El carácter de Información Confidencial es permanente, no está condicionado o limitado a un plazo o término.
2. **Nivel 2: Restringida.** Información con nivel medio de confidencialidad. Esta información estará restringida en su contenido y temporalidad previa evaluación de criterios con base a las leyes o regulada para clases particulares de personas. Se requiere una habilitación formal de seguridad para manejar y acceder a documentos restringidos.
3. **Nivel 3: Interno.** Información con nivel bajo de confidencialidad y de uso exclusivo de la Universidad.
4. **Nivel 4: Pública.** Información de contenidos o documentos de naturaleza pública, cualquiera que sea su formato o soporte, que la Universidad ha publicado y puesto a disposición de todos los usuarios y grupos de interés.

Artículo 6°. Del Programa Institucional de Seguridad de la Información

El Consejo de Coordinación emitirá el Programa Institucional de Seguridad de la Información como instrumento articulador de la presente política con los demás lineamientos institucionales, que será

liderado por la Dirección de Tecnologías de la Información y Comunicación con el acompañamiento del Comité Institucional de Gestión de la Información.

Artículo 7°. Estrategias para la implementación de la política

La presente Política de Seguridad de la Información comprenderá las siguientes estrategias:

1. Definir, implementar, operar y mejorar de forma continua la Gestión de Seguridad de la Información para identificar y gestionar los riesgos sobre los activos de información de La Universidad de La Salle;
2. Definir, mantener y actualizar los requisitos, controles de seguridad, y documentación relacionada, de acuerdo con el contexto de La Universidad.
3. Definir lineamientos, estándares y procedimientos para abordar la seguridad de la información a partir de lo establecido en la presente política.
4. Velar por el mejoramiento continuo de los procesos relacionados con la seguridad de la información inherentes a los activos de información y la declaratoria de aplicabilidad.
5. Definir responsabilidades asociadas a seguridad de la información para el personal y unidades académicas y administrativas que tienen relación con el manejo de los activos de información, garantizando las competencias requeridas para la ejecución de las tareas asignadas;
6. Fomentar una cultura de seguridad de la información en toda la Comunidad Universitaria Lasallista y demás grupos de interés.
7. Comunicar efectivamente los aspectos asociados a los elementos de la Seguridad de la Información a todas las partes involucradas.
8. Incorporar las actividades en materia de seguridad de la información como un componente estratégico en el desarrollo de las funciones sustantivas de La Universidad;
9. Articular procesos y procedimientos relacionados con seguridad, tratamiento y gestión de la información;
10. Cumplir con los requerimientos legales para la seguridad y privacidad de la información, definidos por la normatividad aplicable a La Universidad;
11. Fortalecer la capacidad institucional para asegurar la integridad, confidencialidad, disponibilidad y autenticidad de los activos de información, ante la posible materialización de riesgos.
12. Gestionar los incidentes o eventos de seguridad de la información con las instancias y actores involucrados.
13. Analizar las vulnerabilidades sobre los activos de información de La Universidad de La Salle.
14. Las demás estrategias que sean requeridas para la implementación de la presente política.

Artículo 8°. De los Roles y Responsabilidades

Los roles y responsabilidades para la implementación de la presente Política y demás lineamientos en materia de Seguridad de la Información corresponde a las siguientes instancias:

1. **Consejo Superior.** Aprobar las actualizaciones de la Política General de Seguridad de la Información.

2. **Consejo de Coordinación.** Velar, hacer seguimiento y adoptar las medidas para la adecuada implementación de la presente política y demás lineamientos de seguridad de la información.

3. **Comité CIGIL:**

    a. Recomendar al Consejo de Coordinación las actualizaciones requeridas de la Política de Seguridad de la Información.
    b. Asesorar a la alta dirección sobre las acciones necesarias para la implementación de la Política de Seguridad de la Información.
    c. Acompañar a las instancias involucradas en la implementación y cumplimiento de la Política General de Seguridad de la Información.

4. **Dirección de Tecnologías de Información y Comunicaciones**

    a. Asumir las funciones de Líder de Seguridad de la información en la Universidad.

b. Planear, asesorar, proponer, operar y administrar la tecnología de información e instrumentar en todo su ciclo de vida los lineamientos dispuestos en esta política.
c. Analizar los incidentes de seguridad de la información y recomendar las acciones por adelantar en articulación con las instancias pertinentes.
d. Implementar las medidas y lineamientos técnicos de seguridad informática, en atención a los controles requeridos.

5. **Dirección de Auditoría Interna.** Analizar en conjunto con la **Dirección de Tecnologías de Información y Comunicaciones, los incidentes de seguridad de la información** en su calidad de Oficial de Protección de Datos Personales, para adelantar las acciones pertinentes.

6. **Dirección de Gestión de Información.** Mantener actualizado en corresponsabilidad con las instancias pertinentes el registro de activos de información.

7. **De las Unidades Académicas y Administrativas.** Asumir el cumplimiento de la presente Política de Seguridad de la Información en el desarrollo de sus funciones en corresponsabilidad con la Dirección de Tecnologías de la Información.

8. **De los Usuarios**

a. Administrar de forma adecuada la información que gestionen y a la que tengan acceso en ejercicio de sus funciones.
b. Participar activamente en las actividades relacionadas con sensibilización, toma de conciencia y capacitación en Seguridad de la Información.
c. Velar por el adecuado manejo de los activos de información a los que por la naturaleza de sus actividades tiene acceso.
d. Informar acerca de cualquier incidente o cualquier riesgo que afecte la Seguridad de la Información.
e. Aplicar los lineamientos de seguridad de la información.

Artículo 9°. Articulación con las Políticas Relacionadas con Gestión de la Información

La presente política está estrechamente articulada con la Política de Tratamiento de Datos Personales y la Política de Gestión Documental para propender por una adecuada seguridad de la información y tratamiento de datos.

Artículo 10. El presente Acuerdo rige a partir de la fecha de su emisión y publicación en el Portal Web de la Universidad y deroga el Acuerdo No. 017 del 5 de diciembre de 2019, emitido por el Consejo Superior y demás normas que le sean contrarias.

Dado en Bogotá, D.C. al primer (1°) día del mes de noviembre de 2024.

Firmado digitalmente por: DIEGO JOSE DIAZ DIAZ
Fecha: 2024.11.01 14:34:58 COT
Razón: Consejo Superior
Ubicación: Universidad de La Salle

Presidente del Consejo Superior

Firmado digitalmente por: SARAY YANEHT MORENO ESPINOSA
Fecha: 2024.11.01 11:59:19 COT
Razón: Secretaría General
Ubicación: Universidad de La Salle

Secretaria General