

CONSEJO SUPERIOR
Acuerdo No. 017 de 2019
(5 de diciembre)

POR EL CUAL SE ACTUALIZA LA POLÍTICA DE SEGURIDAD DE 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 mediante Resolución del Consejo de Coordinación No. 051 del 8 de noviembre de 2005, se adoptaron las Políticas de Seguridad de la Información de la Universidad de La Salle.

Que mediante Resolución de Rectoría 338 de 2018, se implementó el Comité Institucional de Gestión de Información de la Universidad de La Salle, como instancia asesora del Consejo de Coordinación y por conducto de su presidente, se recomendó la actualización de las Políticas de Seguridad de la Información, para presentarla a consideración del Consejo Superior.

Que el Consejo de Coordinación en el marco de sus competencias estatutarias y reglamentarias acogió la propuesta y recomendó presentarla al Consejo Superior para su definición.

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 1º. Actualizar la Política de Seguridad de la Información de la Universidad de La Salle, la cual está contenida en los siguientes artículos:

Artículo 2º. Objeto. La Política de Seguridad de Información de la Universidad de La Salle tiene por objeto asegurar por parte de la Comunidad Universitaria la protección de la información como un activo vital, en términos de integridad, confidencialidad y disponibilidad para la gestión de los procesos académico-administrativos y para la toma de decisiones.

Artículo 3º. Definiciones

- 1. Activos de información:** Es todo activo que tiene información y es necesario para realizar los procesos misionales y operativos de la Universidad, a continuación, se definen los activos de información de la Universidad de La Salle:
 - a. Datos:** Representación de información que pueden ser almacenados y procesados por medio de instrumentos mecanizados o automatizados como equipos de cómputo.
 - b. Base de Datos:** Conjunto de datos organizados y estructurados que permiten el tratamiento de la información. Las Bases de Datos pueden estar en medio físico o electrónico.

- c. **Documentos de Archivo:** Registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones. Los documentos de archivos se encuentran en soportes físicos, electrónicos, audiovisuales y gráficos.
 - d. **Aplicaciones:** Software y sistemas de información que utiliza la Universidad para la gestión de la información, en el desarrollo de sus procesos académicos y administrativos.
 - e. **Personal:** Todos los sujetos vinculados con la Universidad que sean identificados como activo de información.
 - f. **Servicios:** Conjunto de actividades que buscan satisfacer las necesidades de la comunidad universitaria.
 - g. **Tecnología:** Equipos de cómputo, teléfonos, dispositivos móviles, impresoras, sistemas de almacenamiento y otros; utilizados para gestionar la información y las comunicaciones.
 - h. **Instalaciones:** Centros de datos o puestos de trabajo en los que se aloja información.
 - i. **Equipamiento auxiliar:** Activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos.
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. **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.
 5. **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.
 6. **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.
 7. **Comité Institucional de Gestión de la Información de la Universidad de La Salle - CIGIL:** Instancia asesora del Consejo de Coordinación, cuyo propósito fundamental es garantizar la articulación e integración de la información institucional indistintamente de su soporte, orientando sobre buenas prácticas de acceso, circulación, seguridad, calidad, eficacia, y responsabilidad en el uso y gestión de la información, y constituyéndose en la instancia que lidera el análisis y recomendaciones en tal materia.
 8. **Comunidad Universitaria Lasallista:** Grupo de personas conformado por los profesores, empleados administrativos, estudiantes y egresados de la Universidad de La Salle.
 9. **Confidencialidad de la Información:** 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.
 10. **Control Criptográfico:** Técnicas criptográficas diseñadas para confidencialidad, autenticidad e integridad de la información.
 11. **Disponibilidad de la Información:** Es la propiedad o atributo de la información, que garantiza el acceso en el momento, formato, y tiempo que se requiera.
 12. **Líder de Proceso:** Se refiere a aquellos roles, cargos o personas que definen y gestionan cada una de las instancias de un proceso.
 13. **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.

14. **Información institucional:** Información que es insumo y/o resultado de cada uno de los procesos, servicios, procedimientos y actividades ejecutadas en la Universidad de La Salle.
15. **Información institucional sensible:** Se refiere a la información relacionada 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.
16. **Ingeniería Social:** Término usado en seguridad informática para referirse a los métodos utilizados para obtener información de manera ilegal a través de la manipulación de los usuarios.
17. **Integridad de la Información:** Es la propiedad o atributo de la información que hace referencia a que la información debe estar libre de modificaciones por parte de personas, procesos o sistemas que no cuenten con la debida autorización.
18. **Inteligencia de negocio:** 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.
19. **Inventario de Activos de información:** Listado de activos de información clasificados de acuerdo con su nivel de importancia, confidencialidad y valor para la Universidad.
20. **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, transferencia y usos de la información.
21. **Seguridad de la Información:** Gestión realizada a través de políticas, lineamientos y procedimientos para el control y establecimiento de los atributos de calidad, autenticidad, trazabilidad, no repudio, disponibilidad, integridad y confidencialidad en la información.
22. **Seguridad informática:** Gestión de la implementación y mantenimiento de las herramientas y controles establecidos a nivel de hardware, software y organizacional para la seguridad de la información.
23. **Sistema de Información Integrado Lasallista –SIIIL:** Es el conjunto de sistemas de Información articulados que facilitan la gestión de los procesos académicos y administrativos de la Universidad de La Salle.
24. **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.
25. **Usuarios:** Se refiere a todo miembro activo de la Comunidad Universitaria Lasallista que posee acceso, controlado o no controlado, a la información y a los recursos o servicios de información institucionales en la Universidad de La Salle.

Artículo 4º. Ámbito de Aplicación

La presente política aplica en todas las unidades académicas y administrativas, a todos los integrantes de la Comunidad Universitaria Lasallista, incluyendo directivos, administrativos, profesores, estudiantes, egresados, personal de servicios generales, y todo contratista o proveedor de servicios, respecto a todos los activos de información.

Artículo 5º. De los Roles y Responsabilidades

Las responsabilidades que asumen las diferentes instancias en la aplicación de la política de seguridad de la información son las siguientes:

1. **Del Comité CIGIL:** Asesorar al Consejo de Coordinación sobre las acciones necesarias para la implementación de la Política de Seguridad de la Información.

2. **De la Dirección de Tecnologías de Información y Comunicación.** Planear, asesorar, proponer, operar y administrar la tecnología de información e instrumentar en todo su ciclo de vida los lineamientos dispuestos en esta política.
3. **Del Grupo de Seguridad Informática.** Implementar los lineamientos necesarios de seguridad informática.
4. **Del Grupo de Seguridad de Información.** Tramitar los incidentes de seguridad e informar al Comité CIGIL la estadística de incidentes.
5. **De las Unidades Académicas y Administrativas.** Asegurar el cumplimiento de esta Política de Seguridad de la Información por parte de todos sus colaboradores.
6. **De los Usuarios.** Administrar de forma adecuada la información que gestionen y a la que tengan acceso en ejercicio de sus funciones.

Artículo 6°. Del Instrumento Articulador de la Presente Política.

Se crea el Programa de Seguridad de Información Institucional, como instrumento articulador de la presente Política, su desarrollo se realizará en un tiempo máximo de un (1) año posterior a la publicación del presente acto administrativo y tendrá los siguientes componentes:

1. Diagnóstico del estado actual de la seguridad de la información en la Universidad.
2. Procedimientos de seguridad de la Información de acuerdo al contexto y nivel de madurez de la Universidad.
3. Roles y responsabilidades en cuanto a seguridad de la información.
4. Inventario de Activos de Información.
5. Mapa de Riesgos de Seguridad de la Información, clasificación y tratamiento.
6. Articulación con el Programa Integral de Gestión de Datos Personales, el Proceso de Gestión Documental, la Política Ambiental.
7. Articulación con el Modelo de Gobierno de la Información que se diseñe en la Universidad.
8. Plan de capacitación y sensibilización en cuanto a seguridad de la información.
9. Responsabilidades a desarrollar por los líderes funcionales de los sistemas de información y la Dirección de Tecnologías de Información y Comunicación para lograr la armonía y adecuada interrelación entre los sistemas de información académicos y administrativos de la Universidad de La Salle.
10. Responsables en cuanto a la seguridad en Centros de Gestión, Centros de Datos y Cuartos Eléctricos.
11. Plan de Continuidad de Operación de la Universidad.
12. Sistemas de monitoreo y detección para identificar de manera temprana los posibles incidentes de seguridad de la información.
13. Procedimientos para el tratamiento de incidentes de seguridad de la información.
14. Plan de implementación del Programa de Seguridad de la Información.
15. Indicadores de Gestión.
16. Plan de Auditorías, Monitoreo y Control.
17. Plan de Mejoramiento continuo de seguridad de información.

Parágrafo. El Consejo Superior, encomienda al Consejo de Coordinación, para que adelante las acciones y fije los procedimientos necesarios para garantizar la adecuada implementación del Programa de Seguridad de Información Institucional, entre ellos, los requisitos para el control de acceso, políticas de correo institucional, y demás determinaciones necesarias para el cabal cumplimiento de lo dispuesto en el presente acto. Se podrá designar un responsable de liderar el Aseguramiento de la Información Institucional si en el proceso de implementación de la presente política se identifica esta necesidad.

Los documentos, relacionados con procedimientos, instructivos, guías, y demás instructivos, que se originen a partir de la implementación de la presente política, deberán quedar formalizados en el Sistema de Gestión de Calidad.

Artículo 7°. De los Administradores de los Inventarios de los Activos de Información

Actuarán como administradores de los inventarios de los Activos de Información las siguientes áreas:

No.	Tipo de Activos de Información	Administrador del Inventario de Activos de Información
1	Datos y Bases de Datos Electrónicas	Dirección de Tecnologías de Información y Comunicación.
2	Bases de Datos Físicas y Documentos de Archivo	Dirección de Gestión de Información.
3	Aplicaciones	Dirección de Tecnologías de Información y Comunicación.
4	Personal	Dirección de Gestión Humana.
5	Servicios	Áreas responsables de la prestación de servicios internos y externos.
6	Tecnología	Dirección de Tecnologías de Información y Comunicación y Dirección de Compras, Inventarios y Activos.
7	Instalaciones	Dirección de Tecnologías de Información y Comunicación y la Dirección de Infraestructura.
8	Equipamiento Auxiliar	Dirección de Tecnologías de Información y Comunicación y Dirección de Compras, Inventarios y Activos.

Parágrafo 1. El inventario de Activos de Información deberá incluir toda la información necesaria para su recuperación en caso de posibles desastres.

Parágrafo 2. Cada activo de información deberá contar con un responsable y se deberán designar responsabilidades específicas, según sea el caso, las cuales deberán registrarse a nivel de área o dependencia responsable.

Parágrafo 3. Todos los Activos de Información adquiridos por la Universidad de La Salle, por sus dependencias, con fines académicos y administrativos, son propiedad de la Universidad de La Salle, así como la información que en ellos se genere, almacene o procese.

Artículo 8°. De la Clasificación de los Activos de Información

Con el objetivo de determinar las estrategias de protección y controles requeridos para la información institucional, se definen los siguientes niveles de clasificación:

- Nivel 1: Confidencial.** Información que tenga datos personales privados, semiprivados y sensibles y demás documentos que, por normas legales y disposición interna, la Universidad determine. Esta información no podrá divulgarse sin el consentimiento expreso de su titular. El carácter de Información Confidencial es permanente, no está condicionado o limitado a un plazo o término.
- Nivel 2: Restringida.** Información utilizada en el ejercicio de la actividad universitaria, y que no ha sido clasificada formalmente como información pública. 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: Pública.** Información de contenidos o documentos de naturaleza pública, cualquiera que sea su formato o soporte, que la Universidad ha puesto a disposición de todos los usuarios o publicada para el uso explícito de la opinión pública. Esta información podrá divulgarse sin autorización del titular u otros.

Artículo 9°. De las estrategias de Seguridad de la Información

La Universidad de La Salle, establecerá las siguientes estrategias para garantizar la seguridad de la información:

1. Establecer el Programa de Seguridad de Información de la Universidad de La Salle.
2. Contar con controles de acceso restringido, para aquella información impresa o electrónica que ha sido clasificada como confidencial o sensible en atención a la Política de Protección de Datos Personales de la Universidad de La Salle y a la clasificación de la Información establecida en el Inventario de Activos de Información y las Tablas de Retención Documental.
3. Implementar un programa de capacitación sobre la seguridad de la Información Institucional.
4. Establecer controles de cifrado, para la protección de la información transportada en medios móviles o removibles, en dispositivos o a través de las líneas de comunicación.
5. Implementar controles criptográficos con el objetivo de proteger la confidencialidad, autenticidad e integridad de la Información Confidencial o Restringida.
6. Establecer lineamientos para la preservación a largo plazo de la información electrónica.
7. Validar con el proveedor del servicio de almacenamiento en la nube, los mecanismos de cifrado de datos que usa y tener siempre el control de las llaves de cifrado.
8. Implementar técnicas de formateo seguro y destrucción de información para el caso de los computadores o dispositivos móviles que van a ser desechados o trasladados a otras dependencias.
9. Garantizar que se destruya la totalidad de los soportes físicos en los procesos de eliminación determinados en las Tablas de Retención Documental-TRD y conforme a los procesos establecidos por Gestión Ambiental.
10. Seguir los lineamientos establecidos en las Políticas de Tratamiento de Información Personal y Gestión Documental de la Universidad de La Salle.
11. Establecer, a nivel contractual, las cláusulas de seguridad de la información y el conocimiento y consentimiento en cuanto a la lectura y conocimiento del documento de la presente política por parte de los colaboradores de la Universidad.
12. Crear lineamientos para la seguridad de los equipos de cómputo o dispositivos móviles que salen de la Universidad para uso académico o administrativo.

13. Las demás, que sean necesarias en el cumplimiento de lo legal, de lo dispuesto en este acto y según lo determinado por el Consejo de Coordinación.

Artículo 10. Licencias de Software

La Universidad de La Salle, atenderá los lineamientos dispuestos en la normatividad vigente de Derechos de Autor y uso de licencias de software. Anualmente se realizará un informe con el estado del licenciamiento de software de la Universidad.

Artículo 11. De los Derechos de los usuarios de la Información Institucional

Son derechos de los usuarios de la Información Institucional:

1. Recibir inducción sobre los Sistemas de Información existentes en la Universidad de La Salle.
2. Conocer los Sistemas de Información que debe emplear para el desarrollo de sus funciones y recibir capacitación para su acceso, uso y consulta.
3. Los asignados por Ley.

Artículo 12. De los Deberes de los usuarios de la Información Institucional

Son deberes de los usuarios de la Información Institucional:

1. Mantener bajo medidas de seguridad la información impresa y la contenida en medios extraíbles en caso de ausencia temporal.
2. Almacenar la información institucional en los equipos de cómputo, medios tecnológicos y espacios asignados por la Universidad.
3. Realizar entrega al Jefe Inmediato de equipos de tecnología a cargo y de información institucional mediante el diligenciamiento de formato de Movimientos de Activos e Inventario Documental en caso de traslado o desvinculación de la Universidad.
4. Garantizar que al entregar o hacer devolución de un computador o dispositivo móvil que le haya sido asignado en ejercicio de sus funciones, no se exponga información de acceso confidencial o restringido.
5. Cumplir con el procedimiento establecido para el movimiento de activos y control de inventario, conservando la trazabilidad del activo manteniendo actualizado el registro del colaborador responsable.
6. Asegurar la destrucción física, antes de ser desechados, de todos los dispositivos que sean discos portables no reutilizables, CDs, DVDs, Blu-Rays para evitar que información pública sea expuesta, previa valoración por parte de la Dirección de Gestión de Información y de acuerdo a los lineamientos establecidos por Gestión Ambiental.
7. Responsabilizarse de la asignación de usuarios y contraseña y uso de la información institucional a la cual tenga acceso.
8. Los demás, que la Ley y normas reglamentarias le impongan.

Artículo 13. De las prohibiciones en el uso de la Información

Se prohíbe todo lo que se considere ilegal que afecte el buen nombre de la Universidad de La Salle y que sea contrario al cumplimiento legal o normativo vigente en cuanto a protección de datos personales, derechos de autor, marcas comerciales, patentes o licencias, y toda conducta contraria que conlleve a la violación de otros derechos.

Artículo 14. Requisitos para el Control del Acceso

Las normas establecidas para el control de acceso deberán considerar los siguientes requisitos: Gestión de acceso a usuarios, registro de usuarios, gestión de privilegios, revisión y mantenimiento de privilegios, matriz de cargos, roles y permisos, desvinculación y cambio de funciones de colaboradores, gestión de acceso al sistema operativo, gestión de acceso remoto, usuarios en teletrabajo y responsabilidad de los usuarios.

Artículo 15. Cuenta y Contraseña Institucional

La Universidad de La Salle ha dispuesto que todos los administrativos, profesores, estudiantes y egresados tengan una cuenta institucional asociada a los servicios que la Universidad considere pertinentes; es así como la cuenta institucional se establece como Identificador Único de cada usuario.

Parágrafo. Existirán excepciones de mantenimiento de la cuenta y contraseña institucional de acuerdo a los casos específicos que se analicen en el Comité Institucional de Gestión de Información de la Universidad de La Salle – CIGIL.

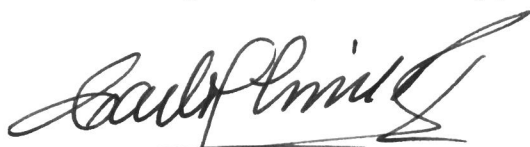
Artículo 16. De la Política de Correo Institucional.

El correo electrónico de la Universidad de La Salle es un servicio que ofrece la Universidad a sus profesores, estudiantes, egresados, administrativos y personal de servicios generales, como herramienta esencial para el desarrollo de sus actividades, y corresponde a la Dirección de Tecnologías de Información y a la Dirección de Comunicación y Mercadeo, según sus competencias, velar por la observancia de administración y gestión de los correos electrónicos institucionales, acorde con lo establecido por el Consejo de Coordinación.

Artículo 17. Las unidades académicas y administrativas que, por decisión institucional, cambien de denominación, asumirán las responsabilidades designadas mediante el presente Acuerdo.

Artículo 18. El presente Acuerdo rige a partir de la fecha de su publicación en el Portal Web de la Universidad y deroga la Resolución del Consejo de Coordinación No. 051 de 8 de noviembre de 2015 y demás normas que le sean contrarias.

Dado en Bogotá D.C., a los cinco (5) días del mes de diciembre 2019.



CARLOS GABRIEL GÓMEZ RESTREPO, f.s.c.
Presidente del Consejo Superior



SARAY YANEHT MORENO ESPINOSA
Secretaria General