

**ESEIT- ESCUELA SUPERIOR DE EMPRESA, INGENIERÍA Y TECNOLOGÍA
ACUERDO CONSEJO DIRECTIVO No. 185
06 DE AGOSTO DE 2021**

Por medio del cual se adopta la POLITICA DE SEGURIDAD DE DATOS DE ESEIT -
ESCUELA SUPERIOR DE EMPRESA, INGENIERÍA Y TECNOLOGÍA

Mediante Acta No. 85 del seis (06) de agosto de dos mil veintiuno (2021), el Consejo Directivo de ESEIT- ESCUELA SUPERIOR DE EMPRESA, INGENIERÍA Y TECNOLOGÍA en ejercicio de las atribuciones legales y estatutarias, y

CONSIDERANDO:

Que la Constitución Política, en su artículo 69, consagra la autonomía Universitaria permitiendo que las instituciones de Educación Superior (IES) puedan darse sus directivas y regirse por sus propios estatutos, de acuerdo con la ley.

Que mediante la Ley 30 de 1992, el Gobierno Nacional desarrolló el derecho constitucional de la autonomía universitaria, estableciendo los parámetros de la misma para las Instituciones de Educación Superior.

Que la Ley 30 de 1992 en su artículo 28, reconoce el derecho de las universidades a crear, organizar y desarrollar sus programas académicos, definir y organizar sus labores formativas, académicas, docentes, científicas y culturales.

Que mediante Resolución número 4787 del 8 de mayo de 2012 del Ministerio de Educación Nacional otorgó a la ELITE ESCUELA LATINOAMERICANA DE INGENIEROS, TECNÓLOGOS Y EMPRESARIOS, hoy ESEIT – ESCUELA SUPERIOR DE EMPRESA, INGENIERIA Y TECNOLOGÍA.

Que mediante Resolución 005037 del 24 de marzo de 2021, el Ministerio de Educación Nacional ratificó el cambio de nombre de ELITE – ESCUELA LATINOAMERICANA DE INGENIEROS, TECNÓLOGOS y EMPRESARIOS al de ESEIT – ESCUELA SUPERIOR DE EMPRESA, INGENIERIA Y TECNOLOGÍA.

Que al tener un cambio de denominación, no afecta su Personería Jurídica, otorgada por Resolución MEN 4787 del 8 de mayo de 2012, ni el código SNIES 9914, ni las condiciones de calidad de sus Registros Calificadas, ni tampoco su NIT 9005345244, en concordancia con la Ley 30 de 1992.

Que en sesión del 22 de junio de 2021, se sometió a consideración del Consejo Directivo en reunión ordinaria con quorum deliberatorio y decisorio la solicitud de adoptar la POLITICA DE SEGURIDAD DE DATOS DE ESEIT - ESCUELA SUPERIOR DE EMPRESA, INGENIERÍA Y TECNOLOGÍA, la cual fue aprobada de forma unánime.

En mérito de lo expuesto,

ACUERDA:

Artículo Primero: Adoptar la POLITICA DE SEGURIDAD DE DATOS DE ESEIT - ESCUELA SUPERIOR DE EMPRESA, INGENIERÍA Y TECNOLOGÍA, documento que se encuentra anexo y hace parte integral del presente Acto.

Artículo Segundo: Remítase copia del presente Acuerdo a la Rectoría y a la Coordinación Académica para los fines pertinentes.

COMUNÍQUESE Y CÚMPLASE

Dado a los seis (06) días de agosto del año dos mil veintiuno (2021)



PLANETA DE AGOSTINI FORMACION Y UNIVERSIDADES HOLDING

Presidente del Consejo Directivo
GUILLERMO USECHI VELATEGUI
APODERADO



HÉCTOR JULIÁN GARCÍA MENDOZA
Secretario General



Política de Seguridad de Datos y Recursos Informáticos de la Escuela
Superior de Empresa, Ingeniería y Tecnología - ESEIT

Acuerdo 185 del 06 de agosto de 2021

Introducción

La Escuela Superior de Empresa, Ingeniería y Tecnología – ESEIT como entidad de educación busca en establecer el buen uso de los datos en las diferentes áreas de la institución. Además, está dispuesta a la protección de los datos e información suministrada por los diferentes miembros que la conforman (Colaboradores, Docentes, Estudiantes y Público en general). De acuerdo a los compromisos de la institución se enfoca en la importancia de la información y en la aplicabilidad de los mismos en los diferentes de medios de apoyo de las actividades académicas de ESEIT.

La Escuela Superior de Empresas, Ingeniería y Tecnología brinda a la comunidad está la política de protección de datos personales señaladas en la Ley N ° 1581 de 2012 y su decreto reglamentario.

Definiciones

Las siguientes son las definiciones consagradas en la **Ley 1581 de 2012**, que permitirán conocer el desarrollo de cada uno de los temas planteados en el presente documento:

- a) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
- b) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento;
- c) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;
- d) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;
- e) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;
- f) **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento;
- g) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Principios

La Escuela Superior de Empresas, Ingeniería y Tecnología conforma su Política de Datos Personales en relación de los siguientes principios:

- a) **Principio de finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, en relación a las diferentes actividades académicas por parte de la institución.
- b) **Principio de libertad:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización.
- c) **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- d) **Principio de transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernen.
- e) **Principio de seguridad:** Se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- f) **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento.

Derechos de los Titulares

Los Titulares de datos personales que reposen en las bases de datos de la Escuela Superior de Empresas, Ingeniería y Tecnología, tienen los siguientes derechos:

- a) **Derecho a conocer, actualizar y rectificar sus datos personales** frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
- b) **Derecho a solicitar prueba de la autorización:** Los titulares de datos personales pueden solicitar prueba de autorización para procesar sus datos, según el artículo 9 de la Ley N ° 1581 de 2012, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley.

- c) **Derecho a ser informado sobre el uso de los datos personales** por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- d) **Derecho a revocar la autorización y/o solicitar la supresión del dato** cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales otorgados a la Escuela Superior de Empresas, Ingeniería y Tecnología – ESEIT.
- e) **Derecho a acceder a los datos personales:** Los titulares de los datos personales se le permitirá de forma gratuita ingresar a sus datos personales que hayan sido objeto de Tratamiento.

Autorización

Los titulares de los datos personales pueden autorizar a la Escuela Superior de Empresas, Ingeniería y Tecnología para abordar a los mismo de cualquier manera que pueda ser objeto de consulta posterior.

Desde cualquier área correspondiente de la escuela superior ESEIT que necesite datos de un titular, al momento de solicitar la autorización, deberá informarle de manera clara y expresa lo siguiente:

- a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo, ante los procesos de académicos o sociales de la escuela superior ESEIT.
- b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.
- c) Los derechos que le asisten como Titular.
- d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Casos en que no es necesaria la autorización

Conforme a lo estipulado en el artículo 10 de la Ley 1581 de 2012, la autorización del Titular no será necesaria cuando se trate de:

- a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- b) Datos de naturaleza pública.
- c) Casos de urgencia médica o sanitaria.

- d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- e) Datos relacionados con el Registro Civil de las Personas.

Deberes del responsable del tratamiento

La Escuela Superior de Empresas, Ingeniería y Tecnología – ESEIT como Responsable del Tratamiento de los datos personales, presenta los siguientes deberes a su cargo:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
- c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- f) Actualizar la información, respecto de los datos previamente suministrado por parte de los titulares con el fin a esta se mantenga actualizada.
- g) Rectificar la información cuando sea incorrecta por parte de los titulares de los datos, en un periodo de 5 días hábiles.
- h) Llevar a cabo de forma oportuna la actualización, rectificación o supresión de los datos en conformidad con lo previsto en la ley 1581 de 2012.

Deberes de los encargados del tratamiento

Son responsabilidad de las personas físicas o jurídicas, que representan a la **Escuela Superior de Empresas, Ingeniería y Tecnología – ESEIT**, tramitar la base de datos personal, como responsable del tratamiento, lo siguiente:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Mantener la información en las condiciones de seguridad necesarias para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos estipuladas por la Ley N ° 1581 de 2012.

- d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- e) Evitar la difusión de información controvertida por parte del titular en los términos señalados por la Ley N ° 1581 de 2012.

Atención a los titulares

La **Escuela Superior de Empresas, Ingeniería y Tecnología – ESEIT** será responsable de seguir las solicitudes, consultas y reclamos, presentados por los titulares de los datos personales a través de cualquiera de los siguientes canales, atendiendo los requisitos de consultas y reclamos establecidos en el punto 10 de la Ley 1581 de 2012.

- Vía Telefónica a través de la Línea nacional: PBX: 061-9140009 / 3330333464
- Mediante solicitud por escrito radicado en la dirección: Carrera 11 # 80-57 Bogotá D.C
- A través del correo electrónico: contacto@eseit.edu.co

Procedimientos

De conformidad con lo dispuesto en la Ley 1581 de 2012, **ESEIT** ha implementado los siguientes procedimientos:

Consulta: El titular o sus causahabientes puede consultar la información personal del titular en la base de datos. **ESEIT** deberá facilitarles toda la información contenida en el formulario de registro personal o relacionada con la identidad del titular.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Reclamos: El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán presentar un reclamo ante la **Escuela Superior de Empresas, Ingeniería y Tecnología**, el cual será tramitado bajo las siguientes reglas:

- El reclamo se formulará mediante solicitud dirigida a la **Escuela Superior de Empresas, Ingeniería y Tecnología**.
- Documento de identificación del Titular.
- Descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

2. RECURSOS INFORMÁTICOS

1. INTRODUCCIÓN

Estas políticas aquí descritas han tenido como objetivo definir una estructura normativa que permita a la Comunidad universitaria hacer el mejor uso posible de los recursos de tecnología, que permita promover los objetivos de ESEIT en un ambiente seguro y claro. Con la implementación de estas políticas, se busca además, preservar la integridad de los recursos informáticos como computadores, redes, sistemas de información, programas y datos propiedad de ESEIT, aun cuando no se encuentren en sus instalaciones; asegurar que el uso de estos recursos cumpla con las leyes, normas y procedimientos legales y de la Institución; proteger a ESEIT de daños a su infraestructura o legales, como consecuencia del uso indebido de los recursos informáticos; entre otros aspectos.

Es importante entender que con el uso de los recursos informáticos, se da aceptación a las políticas de manera automática, por esto es importante que cada persona revise las

mismas y su compromiso con el apoyo al funcionamiento adecuado de los recursos informáticos.

2. ALCANCE

La información es uno de los principales activos de **ESEIT - Escuela Superior de Empresa, Ingeniería y Tecnología**, en adelante **ESEIT**. La información referida a clientes, socios, proveedores, procesos y empleados es crítica para el éxito de ESEIT. Por lo tanto, la protección de esta información es un elemento fundamental para la Institución.

Este documento pretende asegurar un ambiente de funcionamiento que proteja con eficacia la información y los recursos informáticos a través de los cuales la misma se genera, se almacena o se transmite.

La Política General de Recursos Informáticos se basa en las piedras angulares de la seguridad de la información: confidencialidad, integridad, disponibilidad, confiabilidad y responsabilidad.

Es responsabilidad de todos comprometerse con las iniciativas de seguridad de la información. Particularmente el Consejo Directivo y la Rectoría tienen un papel importante en asegurar la seguridad de la información en su área, y para ello, el correcto uso de los recursos informáticos.

3. NORMAS Y POLÍTICAS DE USO DE LOS SERVICIOS IT

Con el fin de regular la utilización de todos los servicios y recursos informáticos que son propiedad de ESEIT es que se establece la Política General de Recursos Informáticos (uso de los servicios IT) para poder así asegurar una óptima calidad de servicio en el cumplimiento de las funciones que desarrolla la Institución.

La comprensión de las responsabilidades que acompañan el uso de la información y de los recursos informáticos de ESEIT, es importante para todos los usuarios que acceden a los sistemas.

La presente política se aplica a todos los sectores de ESEIT, alcanza a todos los empleados y estudiantes, así como recursos externos que requieran estas herramientas para el desarrollo de sus tareas, y regula toda la información creada, almacenada y transmitida electrónicamente a través de los sistemas de ESEIT.

Quedan comprendidos como bienes y recursos informáticos de ESEIT: los suministros y equipos (computadores, periféricos, teléfonos, centro de copiado, etc.); las estaciones de trabajo, las notebooks, los dispositivos móviles y de almacenamiento; el correo electrónico e Internet; los sistemas informáticos y los aplicativos específicos, entre otros.

4. USO LEGAL

- ✓ Está prohibido el hostigamiento MAL intencionado de los usuarios de la información y de los recursos informáticos de ESEIT.
- ✓ Se sancionará la destrucción intencional o daño de equipo, software o datos que pertenecen a ESEIT, a sus empleados, estudiantes o a terceros que presten servicios para ESEIT.
- ✓ Está prohibido el acceso a la red de ESEIT utilizando medios que no sean los provistos por la misma para la función específica del empleado o del tercero que preste servicios a ESEIT, o con propósitos que no correspondan a su función específica.
- ✓ Está prohibida cualquier copia, almacenamiento o transmisión no autorizada de material confidencial de ESEIT. Sólo estarán permitidos los accesos provistos y autorizados por el Área de Soporte IT.

5. USO ÉTICO

Los recursos informáticos de ESEIT se deben utilizar de acuerdo con los estándares éticos de la organización que se detallan a continuación:

- ✓ Está prohibido el uso mal intencionado de los servicios de navegación, correo electrónico o mensajería instantánea, de manera que innecesariamente pueda impedir y/o dificultar el desarrollo de las actividades informáticas de los USUARIOS (como, por ejemplo: iniciar comunicaciones electrónicas interactivas o intercambios de correo electrónico, uso excesivo de sistemas de mensajería interactivos, utilidades de red, u otros).
- ✓ Está prohibido el uso de recursos informáticos provistos por la ESEIT para fines personales o temas no relacionados con la misión de la organización.
- ✓ Está prohibida la violación de los acuerdos de licencia de software (Se prohíbe instalar programas no autorizados por el Área de Soporte IT).
- ✓ Está prohibida la violación de la Política General de Recursos Informáticos, las circulares emitidas por el Área de Soporte IT, y los reglamentos internos de la ESEIT en materia de seguridad y recursos informáticos.
- ✓ Está prohibida la violación de la privacidad de otro usuario.

- ✓ Los usuarios deberán tener resguardo de los bienes y recursos informáticos proporcionados por la ESEIT para ser destinados al uso laboral como herramientas de trabajo, y deberán asumir la responsabilidad por el uso adecuado y prudente de los mismos, comprometiéndose a poner en conocimiento al Área de Soporte IT los desperfectos que presenten tales dispositivos, de manera tal que se reparen cuidando las normas de seguridad.

6. USO DE LAS CUENTAS Y/O ACCESOS A LOS RECURSOS INFORMÁTICOS DE ESEIT.

El usuario que debe acceder a los sistemas de la organización recibe una nueva identificación (alta de usuario) y, al firmar el presente documento, declara conocer y aceptar las normas y políticas del uso de los servicios y recursos informáticos, y acepta sus responsabilidades con relación a la administración y uso de la identificación o clave asignada. Las identificaciones y claves son de uso estrictamente personal al usuario que se le asignan y por lo tanto la responsabilidad por el uso correcto o incorrecto de las mismas recae exclusivamente sobre el mismo usuario.

Ningún usuario podrá ceder su identificación ni temporal ni definitivamente a terceros, so pena de incurrir en las sanciones disciplinarias de Ley. En caso de licencia o ausentismo, el responsable del sector deberá solicitar autorización al Área de Soporte IT para otorgar tal acceso.

Es deber de cada usuario asegurarse de cerrar la sesión de trabajo una vez que finalice la utilización de cualquier servicio a fin de que nadie más pueda utilizar su identificación.

7. SEGURIDAD

El usuario es responsable del uso correcto y suficiente de las herramientas de cada sistema informático y debe prever de mantener la seguridad y confidencialidad de la información almacenada en él. Por ejemplo:

- ✓ Las cuentas de equipo, las contraseñas y otros tipos de autorización se asignan a los usuarios individuales y no deben ser compartidos con otros.
- ✓ El usuario debe seleccionar una credencial/contraseña segura y cambiarla con frecuencia.
- ✓ El usuario debe entender el nivel de protección y seguridad de cada sistema (Bloqueos de navegación, antivirus y otros).
- ✓ El usuario debe ser consciente de la existencia y potencial daño de los virus informáticos y tomar medidas para evitar que sea víctima o transmisor involuntario.

- ✓ El usuario debe respetar y en caso de corresponder hacer respetar a sus subordinados, todas las normas relativas a garantizar la seguridad informática del sistema.
- ✓ Queda prohibido proveer información confidencial o sensible a personas no autorizadas, así como ingresar datos falsos o excluir datos correctos en los sistemas.
- ✓ Queda terminantemente prohibido el uso y/o instalación de software no explícitamente autorizado por el Área de Soporte IT. (por ejemplo: freeware, shareware, juegos, programa no licenciados, sistemas de mensajería, etc.)

8. USO DE LA NAVEGACIÓN EN INTERNET.

El servicio de navegación en Internet debe ser utilizado solamente para fines laborales en ESEIT.

Se encuentra terminantemente prohibido el acceso a redes sociales, foros, blogs (salvo para aquellas áreas que expresamente lo autorice el Área de Soporte IT), sitios de venta colectiva, material pornográfico o de contenido obsceno o cualquier sitio cuyo registro puede perjudicar tanto a su persona como a la institución.

El usuario tendrá el conocimiento de que ESEIT se reserva el derecho de supervisión y auditoría sobre los servicios otorgados a los empleados, estudiantes y terceros.

Los usuarios con acceso a Internet deberán cumplir con todas las leyes de propiedad intelectual y restricciones al uso de licencias, debiendo dirigir sus consultas al respecto al sector legal de ESEIT.

Todos los usuarios de Internet por medio de la presente aceptan que el servicio de Internet es un recurso propio de ESEIT y, en virtud de ello, su uso por parte del personal debe ser justificado para cumplir el objeto de la prestación laboral y/o en beneficio de ESEIT, tal como si se tratara de cualquier otro recurso o herramienta provista por ESEIT.

9. USO DEL CORREO ELECTRONICO.

Al utilizar cuentas de acceso para correo electrónico, o bien al identificarse como integrante de ESEIT utilizando una cuenta de acceso adquirida individualmente el usuario deberá dar cumplimiento a las siguientes premisas:

- ✓ Se encuentra prohibido enviar mensajes y/o bajar y/o transmitir cualquier material ajeno a la función laboral y/o la actividad de ESEIT.
- ✓ Se encuentra prohibido el uso de lenguaje obsceno o inadecuado en mensajes.
- ✓ Es deber de los usuarios a quienes se le asignen cuentas revisar el buzón de entrada de su correo con frecuencia, esto con el fin de realizar una administración eficiente del mismo. De igual manera, es su deber eliminar de su buzón de entrada a aquellos mensajes que no necesite mantener almacenados y vaciar frecuentemente la papelera de reciclaje.
- ✓ Es deber de los usuarios velar por no comprometer la buena imagen de ESEIT al identificarse con una cuenta de correo Institucional.
- ✓ No se deben enviar correos tipo SPAM es decir “correo basura”, cadenas o mensajes en serie. No se deben enviar mensajes de correo electrónico alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse.
- ✓ Deberá evitarse, en la medida de lo posible, anexar archivos de gran tamaño en los correos electrónicos de cuentas de usuarios de ESEIT. En caso de ser necesario puede usar los servicios de almacenamiento virtual establecido por ESEIT.
- ✓ Deberá abstenerse de abrir anexos o reenviar mensajes cuyo contenido o procedencia sean dudosos.
- ✓ El usuario tendrá el conocimiento de que ESEIT se reserva el derecho de supervisión y auditoría sobre los servicios otorgados a los EMPLEADOS.
- ✓ Todos los usuarios del correo electrónico por medio de la presente aceptan que el correo electrónico es un recurso propio de ESEIT y, en virtud de ello, su uso por parte del personal, debe ser justificado para cumplir el objeto de la prestación laboral y/o en beneficio de ESEIT, tal como si se tratara de cualquier otro recurso o herramienta provista por ESEIT.

10. USO DEL ESPACIO DE ALMACENAMIENTO PERSONAL EN LOS SERVIDORES Y EN LAS ESTACIONES DE TRABAJO

El usuario no debe exceder la capacidad de almacenamiento asignada para la utilización de los servicios informáticos. El usuario será responsable del perjuicio que pueda ocasionarle el no poder recibir, ni almacenar más archivos en caso que llegue a su máximo espacio asignado.

El espacio de almacenamiento será utilizado solamente para guardar información de carácter operativo, administrativo y de desarrollo. Cualquier información almacenada que no sea acorde con lo anterior (música, videos, virus, programas maliciosos, etc.), podrá ser removida sin previa consulta con el usuario.

Se realizarán revisiones periódicas sobre el buen uso del espacio asignado por parte del Área de Soporte IT.

11. USO DE LAS ESTACIONES DE TRABAJO Y/O DISPOSITIVOS MÓVILES.

Los usuarios deben velar por la conservación de las estaciones de trabajo, dispositivo móvil o cualquier otro equipamiento utilizado dentro o fuera de ESEIT.

No se deben realizar modificaciones en la configuración de los equipos instalados.

Si algún implemento o estación de trabajo puesto para su servicio es dañado por un mal uso o negligencia grave, el costo del arreglo o valor en caso de pérdida, deberá ser asumido por el usuario que lo ocasione.

Se prohíbe el uso de dispositivos personales dentro del ámbito de ESEIT salvo excepciones autorizadas por parte del Área de Soporte IT.

12. DERECHOS DE ESEIT

Los sistemas de correo electrónico son de propiedad de ESEIT y los archivos que se encuentran almacenados en los mismos constituyen información privada y de propiedad de ESEIT.

El ingreso a páginas web o el envío de correos electrónicos cuyos contenidos no respondan a fines funcionales para cumplir el objeto de la prestación laboral, será considerado como una falta grave a la presente política de ESEIT.

ESEIT se reserva el derecho de auditar, revisar y analizar todos y cada uno de los datos, información y actividades en las estaciones de trabajo y otros dispositivos electrónicos facilitados por ESEIT a los usuarios; a los efectos deberá tenerse en consideración la legislación nacional vigente y, en particular, respecto de la preservación del derecho de privacidad. Asimismo, ESEIT se reserva el derecho de supervisar o revisar el uso de los recursos provistos a los Trabajadores sobre los servicios de internet y correo electrónico, así como de otras comunicaciones electrónicas, circunstancia que es debidamente informada a los usuarios a través del presente documento. Esta información puede y será utilizada en el proceso de recolección de evidencia de acciones no autorizadas o violaciones a las políticas establecidas por ESEIT.

Los permisos de acceso podrán ser revocados en cualquier momento si se verificasen conductas impropias y/o abusivas de los usuarios.

13. DEBERES Y OBLIGACIONES DE DIRECTORES, SUBDIRECTORES O SUPERVISORES DE ESEIT

Cada persona a la cual se le hubiera asignado una computadora de escritorio y/o portátil será responsable de la misma. Sin perjuicio de ello, las personas con cargos de gerente, jefe o supervisor deberán:

Definir y justificar la necesidad de uso de los recursos informáticos que requiera el personal a su cargo.

Monitorear su utilización y la aplicación efectiva en el desarrollo de las tareas de los usuarios autorizados.

14. DEBERES Y OBLIGACIONES DEL PERSONAL DE SISTEMAS

- ✓ Deberá instrumentar las acciones operativas relacionadas con esta normativa.
- ✓ Deberá informar a las Direcciones, Subdirecciones u otras dependencias los desvíos detectados para los usuarios que corresponda.
- ✓ Deberá responder a las solicitudes realizadas por el Consejo Directivo, otras dependencias autorizadas y Rectoría de ESEIT, con respecto al uso que cualquier usuario haya hecho de las herramientas informáticas objeto de esta norma.

15. ELEMENTOS DE RESPALDO.

Los elementos de respaldo o Backup son los repositorios con lo que cuenta ESEIT para guardar la información. Estos corresponden a ubicaciones físicas y en la nube que son de fácil acceso, manipulación y son confiables para guardar la información, que en caso de un evento requiera recuperar de ESEIT para continuar con su funcionamiento.

- ✓ Discos externos, se cuenta con 5 discos externos cada uno de 1 TB de capacidad, que contiene la información de los equipos de cómputo y OneDrive, así como una copia de aplicaciones como SIIGO (una vez instalado).
- ✓ OneDrive, ESEIT cuenta con este aplicativo que suministra un espacio de almacenamiento de 1 TB por usuario y permite salvaguardar la información de las diferentes áreas en línea.

16. APLICATIVOS QUE SE RESPALDAN.

Para establecer el correcto funcionamiento de ESEIT, se deben realizar actividades específicas sobre los siguientes aplicativos misionales.

- ✓ Sistema Académico - Q10: Es nuestra plataforma académica, sobre este se realizan todas las actividades de procesos como admisiones de alumnos, programación de los encuentros, grabación de los encuentros sincrónicos mediante plataforma ZOOM, registros de notas e historial académico de los alumnos. Este software funciona bajo la modalidad de cloud, por lo tanto, el proveedor respalda la información.
- ✓ SIIGO: Software contable y administrativo, se encarga de los procesos contables, financieros, tributarios. Se encuentra instalado en un computador del área contable, mecanismo de Backup es generado a Disco Duro Externo.
- ✓ HECAA: Software del ministerio de educación para el reporte de información, este software funciona bajo la modalidad de cloud, por lo tanto, el proveedor respalda la información.
- ✓ Blackboard: Es una plataforma educativa que utiliza una conexión a Internet para brindar acceso a los cursos desde un lugar remoto, de una manera flexible y sencilla para profesores y estudiantes con una cuenta institucional, mecanismo de Backup es generado a Disco Duro Externo.

17. EVITAR HACER TRAMPA EN LA PRESENTACIÓN DE ACTIVIDADES EVALUATIVAS DE FORMA VIRTUAL

Al crear un cuestionario o examen online, nuestro campus Blackboard nos brinda una variedad de opciones para promover la honestidad y la integridad académica en las presentaciones de estas actividades, estas funciones son las siguientes:

- ✓ Configurar el examen para mostrar una pregunta a la vez
- ✓ Prohibir el retroceso
- ✓ Usar varios tipos de preguntas e incluir preguntas abiertas
- ✓ Asignar fechas para el examen
- ✓ Establecer temporizador
- ✓ Esconder los resultados
- ✓ Intentos múltiples
- ✓ Preguntas en orden aleatorio

Estas funciones pueden ayudar a prevenir las trampas en los exámenes en línea al detectar intentos de trampa o identificar patrones persistentes de comportamiento sospechoso.

Esto añade un componente humano a la tecnología para eliminar las estrategias de trampa.

- ✓ Realizar las actividades tipo evaluativo (exámenes o quices) en vivo
- ✓ Encender cámara mientras realiza la actividad
- ✓ Verificar la identidad de los participantes.

Nota: Estas estrategias deben ser aprobada por el área académica e informada con los estudiantes con el fin de evitar controversia o problemas futuros.

Este documento hace parte del Acuerdo 185 del 06 de agosto de 2021