TECNOLÓGICO DE ENERGÍA E INNOVACIÓN

CONSEJO SUPERIOR

Acuerdo No. 002 del 27 de enero de 2020

Por medio del cual se actualiza la política de Seguridad de la información del TECNOLÓGICO DE ENERGÍA E INNOVACIÓN E-LERNOVA:

CONSIDERANDO

Que su gestión está regida principalmente por la Ley 30 de 1992, la Ley 115 de 1994 y el Decreto Único Reglamentario 1075 de 2015 del Sector Educativo

Que E-LERNOVA adoptó una política de la seguridad de la información teniendo en cuenta que la información de su operación es un activo muy valioso y que debe ser protegido y regulado al interior de la Institución, y que la dinámica institucional requiere de la actualización de ésta política para incluir nuevas estrategias en la materia

Y que de acuerdo con el Plan de Desarrollo Institucional se adopta un nuevo sistema de información académico administrativo,

RESUELVE

Artículo 1: Actualizar la política de seguridad de la información en E-LERNOVA con las pautas del buen manejo de la información institucional

COMUNIQUESE, PUBLIQUESE Y CUMPLASE

Dado en Chía, el día 27 de enero de 2020

RICARDO STRIEDINGER CEPEDA
Presidente Consejo Superior

SAMUEL STRIEDINGER MELO
Secretario General Consejo Superior

1. POLITICA

"La información es la moneda global y por consiguiente un activo de muy alto valor para el cumplimiento de los objetivos misionales de E-LERNOVA, por lo que es necesario establecer lineamientos que consoliden una cultura de seguridad y confidencialidad de la información en E-LERNOVA que fundamentada en los siguientes objetivos:

- Proteger la información de cada miembro de la comunidad institucional.
- Asegurar la protección de la información referente a contenidos, cursos, datos personales, e-portafolios, calificaciones y demás elementos del repositorio tanto del personal administrativo como estudiantil alojado en las plataformas académicas y administrativas.
- Crear estrategias de socialización y recordación de prácticas seguras para mantener nuestro campus virtual libre de ciberataques de ante posibles hackers.
- Reconocer las políticas y definir procedimientos de seguridad de la información y gestión de la información física y electrónica.
- Compromiso institucional para el buen manejo de la información de tal forma que se minimicen los riesgos de: revelación, alteración, violación o borrado de la misma, así como mantener los recursos tecnológicos para el normal desarrollo de las actividades académicas y administrativas, alineado co el sistema de gestión de la información que se implemente en E-LERNOVA.
- Aplicar los cuatro pilares de la seguridad informática y manejo de la información:

    - Disponibilidad: que la información esté siempre disponible teniendo en cuenta las variables de tiempo, lugar y oportunidad.
    - Confidencialidad: que solo sea accedida por las personas o sistemas autorizados y que en su trasmisión no sea interceptada.
    - Integridad: que no sea modificada ni en su almacenamiento o trasmisión.
    - No repudio: garantizar que no se pueda negar algo que se hizo en los sistemas de información, archivos y demás información que está en medio digital.

Se considera información para efectos de la política lo dicho o escrito, informes, conocimiento y datos, que se comunican o transmiten por medios orales y escritos incluyendo los electrónicos. El responsable de la información es quien emite o recibe la información propia de su rol o cargo y que se constituye en un insumo para cumplir con el objetivo de sus funciones y tiene la responsabilidad de administrarla de acuerdo con su valor y requisitos. También hay usuarios de la información y son responsables de proteger los activos de información de la institución por

medio del cumplimiento de la política de la seguridad de la información y estar alerta para reportar incumplimientos a la misma.

2. ALCANCE

Todo el personal que integra la comunidad institucional, docentes, administrativos, estudiantes, expertos, directivos, etc., se regirán mediante las políticas de seguridad de la información expresadas en el presente documento.

3. VIGENCIA

El presente documento "*Políticas de la seguridad de la información en E-LERNOVA*" tendrá vigencia hasta ser reemplazado por la siguiente versión revisada y aprobada.

4. INFRAESTRUCTURA TECNOLOGICA

Es el área responsable de revisar y proponer a las directivas institucionales las políticas, lineamientos procedimientos en materia de seguridad de la información, velar por su correcto desarrollo y generar las acciones de formación y estrategias necesarias para consolidar una cultura de seguridad. Representará a la institución en lo referente a la seguridad de la información cuando así sea requerido.

5. ESTRATEGIAS

E-LERNOVA protegerá la información de sus estudiantes y demás personal administrativo y docente mediante sistemas de control administrativo y softwares de seguridad para sus plataformas: Académica (LMS) y Administrativa, mediante las siguientes estrategias:

- Limitar el acceso a funciones específicas e información a través de la asignación de roles basados en permisos en el LMS, software administrativo
- Proveer a la comunidad institucional manuales, procedimientos, instructivos, guías claros y video tutoriales exploratorios para eliminar la necesidad de experticia técnica o la carencia de información.
- Utilizar datos encriptados y procesos confiables de contraseñas aplicados para el ingreso

y codificación de archivos alojados en las plataformas.

- Sistemas encriptados SSL de la información en LMS. Edvance360 provee una red social encriptada que asegura la confidencialidad de la información.
- Cada persona que tenga un acceso a sistemas de información o que manipule información institucional local en los equipos dispuestos para tal fin, deberá firmar un acuerdo de confidencialidad
- No se permite información de tipo personal en los PC y demás herramientas dispuestas por E-LERNOVA
- Se implementará un plan permanente de capacitación y sensibilización a través de los medios de comunicación masiva para consolidar la cultura de seguridad de la información.
- Toda la comunidad debe vigilar el cumplimiento de la presenta política y cuando exista una violación informarla a la dirección de Infraestructura tecnológica.
- La institución contará con un sistema de protección perimetral que proteja la navegación en internet y los mensajes de e-mail contra virus, malware, spam y otros medios de ataque a los sistemas informáticos.
- Elaboración de una guía para la asignación de claves y recomendaciones para su recordación o actualización.
- El área de infraestructura Tecnológica será la única autorizada para instalar o desinstalar software en los Equipos del tecnológico, así como también de recomendar el uso o no uso de aplicaciones o software teniendo en cuenta su naturaleza y características de seguridad en los desarrollos académicos. El control y actualización del software también será responsabilidad de esta área. Dentro de la institución existen tres grandes grupos sobre los cuales se diseñarán los perfiles de usuarios:
  - Personal Académico-Administrativo: Es el personal vinculado contractualmente con E-LERNOVA, para el desarrollo de actividades académicas y/o administrativas que contribuyan al desarrollo de la misión institucional. Según sus funciones y responsabilidades se asignarán permisos de consulta, de gestión o de administración.
  - Personal Docente: Es el personal encargado de desarrollar los módulos que constituyen la oferta académica institucional y/o de acompañar, guiar y facilitar El proceso de enseñanza-aprendizaje de los estudiantes durante su permanencia en E-LERNOVA.
  - Estudiantes: Es el personal que adelanta procesos de aprendizaje a nivel de pregrado o educación continuada. Para adquirir la calidad de estudiante debe cumplir con los parámetros establecidos en el Reglamento Estudiantil.
- El cuidado y protección de los datos de acceso es responsabilidad del usuario, así como las acciones que se realicen en los diferentes sistemas de información bajo dichos datos

de acceso.

- La institución realizará las auditorias técnicas para garantizar el correcto funcionamiento de la plataforma de gestión de aprendizaje y demás sistemas de información de los que disponga.
- Se informará al estudiante antes del inicio de las actividades académicas los requerimientos técnicos y de conectividad para acceder a los contenidos y sistemas información institucionales bajo las recomendaciones del área de infraestructura y soporte y de recursos virtuales en lo que a cada uno corresponde.
- La participación e interacción entre los diferentes actores institucionales deberá desarrollarse en términos respetuosos, cordiales y dentro de las normas de comunicación e-learning.
- La Institución contará con los mecanismos de seguimiento y trazabilidad para determinar los ingresos, actividades, avances y recursos de los estudiantes, docentes y tutores en sus diferentes a la plataforma de gestión de aprendizaje.
- Los estudiantes, docentes y demás personal institucional tendrán a su disposición los manuales, videotutoriales, listado de preguntas frecuentes de las diferentes plataformas y/o herramientas con que cuenta la Institución.
- Se brindará soporte técnico a través del correo electrónico, foros técnicos, vía telefónica, chat de atención en línea, los cuales estarán disponibles durante el desarrollo del período académico.

6. CARACTERISTICAS DE SEGURIDAD DEL SISTEMA DE APRENDIZAJE EN LÍNEA (Plataforma académica)

La LMS utiliza numerosos métodos para mantener un campus seguro para E-LERNOVA. Se rige bajo nuevas tecnologías las cuales se ponen a disposición de la institución, siguen parámetros industriales de seguridad, están actualizadas con el fin de prevenir que un tercer agente pueda acceder sin autorización y así conseguir información confidencial.

Edvance360 regularmente inspecciona todos los aspectos del sistema para asegurar que es resistente a nuevas amenazas, por ello se encuentran en constante actualización de software de seguridad informática, como prueba de ello es el reconocimiento que se les ha otorgado el premio “CODiE ” los cuales son entregados anualmente por la “Software and Information Industry Association” galardonando la excelencia en el desarrollo de software dentro de la industria de TIC.

El centro de datos de Edvance360 es análogo a una fortaleza, posee un equipo de alta seguridad con técnicas y procedimientos que son usados para monitorear y controlar la facilidad.

Adicionalmente Edvance360 monitoria a través de Sistemas de Detección de Intrusión (IDS), SSL, transferencias encriptadas de archivo y software para detección de fallas y reporte proactivo NAGIOS.

6.1 MANTENIMIENTO Y BACKUP DE LA PLATAFORMA EDVANCE360

El sistema de alimentación interrumpida (UPS) de Edvance360 es utilizado para evitar picos de tensión, sobretensiones, y caídas de electricidad, el mantenimiento ocurre a horas planeadas con anticipación y usualmente en un horario de muy bajo tráfico dependiendo de la institución, los backup de información alojada por las instituciones se realizan a diario, semanal y mensual.

6.2 SITUACIONES DE EMERGENCIA

Edvance360 está disponible siempre para una situación de emergencia, generada por desastres o interrupciones eléctricas o de red. Se entiende como "Desastre" cualquier ocurrencia que causa la pérdida de funcionalidad del servidor, y pérdida de la información debido a un desastre de fuerza mayor.
Los servidores de E-LERNOVA y de Edvance360 servers se encuentran alojados en Amazon Web Services.

Los backups institucionales se encuentran en discos externos, dos en las instalaciones de E-lernova custodiados por la persona designada por el Rector y otro a cargo de Vicerrectoría Académica, este último se encuentra a disposición del grupo administrativo, el cual se alimenta a diario.

Además de ello la institución cuenta con almacenamiento en "Dropbox" disponible para los administrativos de la institución, sincronizado en sus computadores para realizar backup de manera sincrónica y en línea.

6.3 SEGURIDAD DE LAS PLATAFORMAS DE SOPORTE ACADÉMICO Y ADMINISTRATIVO

Veamos a continuación las estrategias implementadas en E-LERNOVA para la seguridad del campus virtual:

- Acceso a la información por niveles de permisos.

- Definición de perfiles.
- Asignación y establecimiento de controles de acceso en usuarios
- Asignación de privilegios.
- Implantación de un software de protección contra código malicioso.
- Existencia en la red de datos de dispositivos de seguridad como firewall e IDS.
- Habilitación de filtros de acceso y contenido en internet y en los mensajes de correo.
- Segmentación de las redes de datos y la realización de pruebas de vulnerabilidades técnicas a la plataforma tecnológica.

Para E-LERNOVA el cuidado y protección de la información es una función prioritaria, ya que ésta constituye un recurso invaluable y es el sello representativo de la puesta académica institucional. Por esta razón, debe ser debidamente protegida, garantizando su acceso y disponibilidad a los diferentes estamentos institucionales y minimizando los riesgos de pérdida, hurto, alteración indebida o daño de la misma. En este sentido se establece el procedimiento para atender las solicitudes de creación, modificación y cancelación de cuentas de usuarios.

Se identifican los siguiente medios donde se requiere la asignación de usuarios y contraseñas que permitan el acceso al Sistema de Información Institucional:

1. Sistema de Información Administrativo
2. Sistema de Gestión de Aprendizaje: Edvance360 y aulas virtuales
3. Biblioteca Virtual
4. Correo Institucional

Así mismo, se identifican responsabilidades, se establecen requerimientos mínimos para una adecuada gestión de usuarios, a fin de garantizar la protección, confiabilidad, disponibilidad, difusión y consolidación de la información dentro de la gestión y cultura institucional. La administración de usuarios debe garantizar que cada usuario tenga acceso únicamente a la información que requiere. Criterios:

- Confidencialidad y disponibilidad de la información institucional
- Autorizaciones sean conformes a sus necesidades
- La información por él usuario depositada dentro de los diferentes sistemas de información será salvaguardada bajo los mismos parámetros de seguridad y protección.

Para ello, se define los perfiles de usuarios, estableciendo las necesidades de información y los privilegios que tendrá dentro del Sistema de Información Institucional.

Dentro de la institución existen tres grandes grupos de perfiles de usuarios:

- Personal Académico-Administrativo: Es el personal vinculado contractualmente con E-LERNOVA, para el desarrollo de actividades académicas y/o administrativas que contribuyan al desarrollo de la misión institucional. Según sus funciones y responsabilidades se asignarán permisos de consulta, de gestión o de administración.

- Personal Docente: Es el personal encargado de desarrollar los módulos que constituyen la oferta académica institucional y/o de acompañar, guiar y facilitar el proceso de enseñanza-aprendizaje de los estudiantes durante su permanencia en E-LERNOVA.

- Estudiantes: Es el personal que adelanta procesos de aprendizaje a nivel de pregrado o educación continuada. Para adquirir la calidad de estudiante debe cumplir con los parámetros establecidos en el Reglamento Estudiantil.

RESPONSABILIDADES

La creación de usuarios y contraseñas para acceso de plataformas y biblioteca, se realiza desde el proceso de admisión, registro y control, como responsable del proceso y administración, de acuerdo a los roles: administrador, Docente, Tutor, Estudiante, producción.

Las cuentas de correo institucional serán de responsabilidad del área de infraestructura Tecnológica, quien además consolidará el cuadro control de usuarios y claves de la institución en diferentes aplicaciones y software.

ASIGNACIÓN DE USUARIOS Y CONTRASEÑAS

Los datos de usuario y contraseña permiten la validación y autenticación de la identidad de un individuo para permitir el acceso a los sistemas de información institucional.

- ID Usuario: es el nombre con el cual se podrá ingresar a los diferentes sistemas de información de la institución. La información de los estudiantes (nombres completos y correo electrónico), será obtenida directamente del Sistema de Admisiones y Registros Académico.

- Contraseña: serie de caracteres alfanuméricos que permite el acceso a un usuario

determinado a los diferentes sistemas de información de la institución, Debe ser mínimo de seis dígitos y contener caracteres alfanuméricos.

- La contraseña inicial será el mismo usuario. Los usuarios deberán cambiar su contraseña en su primer procedimiento de identificación.

- El permiso de acceso otorgado a un usuario para el sistema de información institucional, tendrá vigencia hasta la finalización del programa académico o curso.

7. DEBERES DE LOS USUARIOS

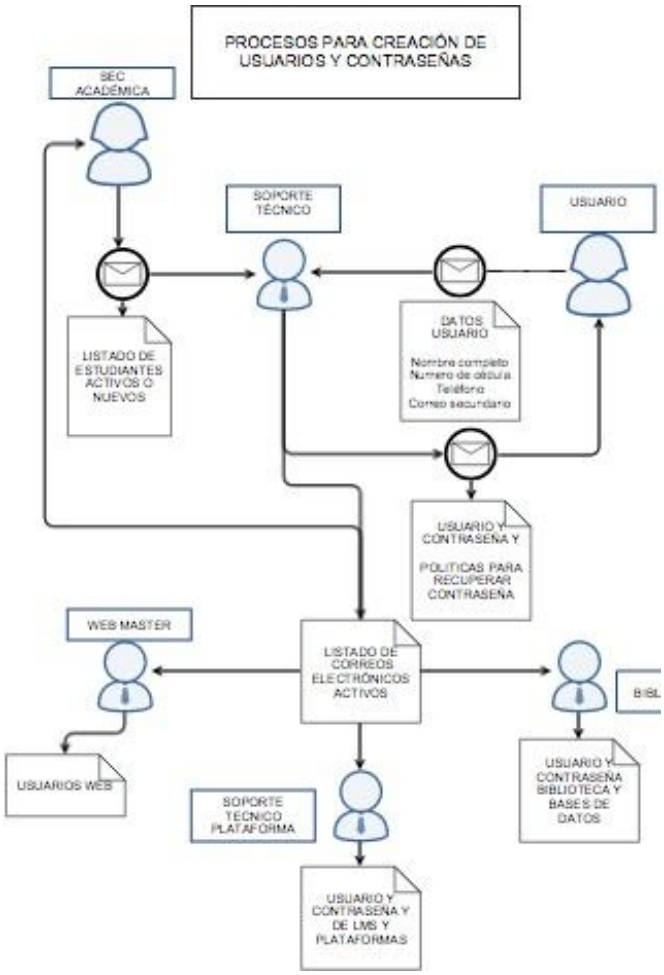
- El usuario y contraseña asignado es de uso personal e intransferible.
- La responsabilidad del usuario modificar su contraseña una vez que ha sido notificada por el administrador.
- El cuidado y protección de los datos de acceso es responsabilidad del usuario, así como las acciones que se realicen en los diferentes sistemas de información bajo dichos datos de acceso.
- Los usuarios son responsables por el uso adecuado de la información a la cual tengan acceso.

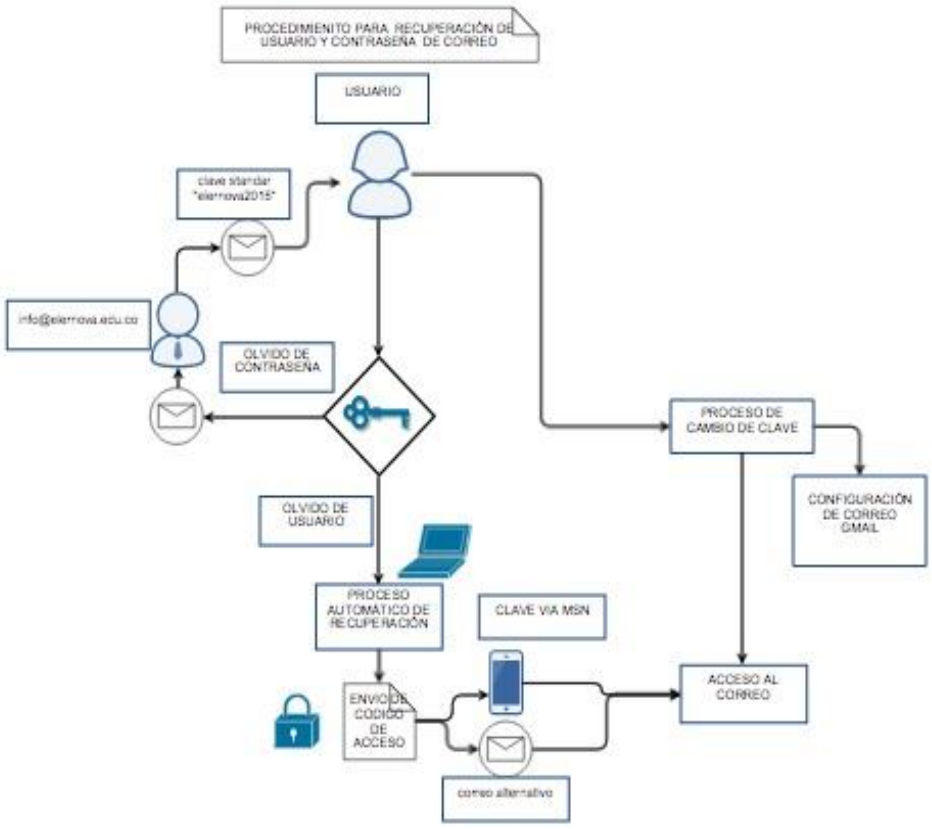
8. MODIFICACIÓN Y CANCELACIÓN DE CUENTAS

La solicitud de modificación y cancelación de cuentas debe realizarse por correo electrónico a al área admisión control y registro, indicando las causas que motivan la solicitud.

A fin de mantener un control eficaz de los usuarios y accesos, al finalizar el semestre se realizará una revisión de derechos de acceso a la base de datos de usuarios activos, con el fin de comprobar que el personal administrativo y docente retirado, al igual que los estudiantes graduados, aplazados o sancionados ya no tengan acceso a los sistemas de información institucionales.

La plataforma administrativa que contiene el sistema de información del estudiante, permite crear a cada estudiante su usuario y contraseña, la cual es informada en el proceso de inscripción, acorde con el siguiente flujograma:





9. ESTRATEGIAS DE SEGURIDAD EN LAS INSTALACIONES FÍSICAS DE E-LERNOVA

Veamos a continuación las estrategias de seguridad en las instalaciones físicas de E-LERNOVA:

- Personal vigilante de las instalaciones físicas de E-LERNOVA todos los días del año.
- Cámaras digitales de cobertura.
- Sistemas de alarma.
- Luz con detección de movimiento.
- Encercado con cerda eléctrica en la periferia de la infraestructura física.
- Sistemas contraincendios.
- Los computadores en las instalaciones de la universidad se encuentran con acceso a través de contraseñas, las cuales han sido parametrizadas para el uso del LMS y SIS.
- Control por invitación verificada de personal que ingresa a las instalaciones de E-LERNOVA.

10. CONTROL DE CAMBIOS

				
1	27-01-20	Actualización general	Calidad y Aseguramiento	Acuerdo 02 del 27-01-2020 Consejo Superior
0	16-02-15	Documento definitivo - Res 04 de 16-02-15	HSEQ	Rector
REV.	**FECHA**	**DESCRIPCIÓN**	**ELABORÓ**	**APROBÓ**