1. OBJETIVO

Establecer los lineamientos mínimos y responsabilidades que deben cumplir todos los usuarios que hacen uso de las aplicaciones institucionales a las que se acceda con usuario y contraseña con el fin de apoyar la confianza y experiencia digital en el uso de este. Adicionalmente, incrementar los beneficios del uso de contraseñas como una herramienta de seguridad, que provee la Universidad para servicio de toda la comunidad Externadista.

2. ALCANCE

Esta política se establece para toda la comunidad universitaria representada por el personal administrativo, docente, estudiantes, egresados, y partes interesadas que hacen uso de contraseñas en las aplicaciones de la Universidad.

El incumplimiento a esta política traerá consigo, las consecuencias que estén previstas en la normatividad vigente y en especial lo previsto en materia de privacidad de la información y la protección de datos personales.

3. NORMAS Y LINEAMIENTOS GENERALES

3.1 GENERALIDADES

El presente documento hace parte del compendio de políticas de seguridad de la información definidas por la Universidad Externado de Colombia; es así como estos lineamientos conforman el Modelo de Seguridad y Privacidad de la Información.

La necesidad de visibilidad y accesibilidad que demanda la cultura digital que hoy día vivimos, hace necesario que la gestión educativa y administrativa de la Universidad se apoye en el uso de recursos tecnológicos para el almacenamiento, procesamiento y transmisión de la información. Esta nueva era de interacciones, interconexiones y agilismo en el ciberespacio trae implícitamente nuevos riesgos que buscan comprometer la confidencialidad, integridad y disponibilidad de la información institucional; la materialización del riesgo en cualquiera de estos pilares puede impactar negativamente a la ciudadanía y a la Universidad como institución.

Los lineamientos establecidos en este documento son el marco de referencia para la implementación de manuales, procedimientos, documentos que deben ser parte fundamental del modelo y que tienen por objeto apoyar la construcción de una arquitectura de seguridad

sustentada en procesos uniformes y buenas prácticas, integrada con la arquitectura TI y con la gestión de controles efectivos, que respondan por la seguridad de la información en la Universidad.

Por consiguiente, la Universidad se ha comprometido con el desarrollo de una estrategia en seguridad de la información que fortalezca y proteja los recursos tecnológicos, con el fin de disminuir el impacto generado sobre la posible vulneración de la información que reposa sobre los mismos; mejorando la confianza y experiencia digital de la Comunidad Externadista cuando hacen uso de los servicios y/o aplicaciones.

3.2 MARCO REGULATORIO

Para el desarrollo de la presente política se han tomado como referencia estándares y metodologías relacionadas con la seguridad de la información que por su naturaleza pueden ser acogidos por cualquier sector industrial e indiferentes al tamaño o enfoque. Es importante aclarar que, con excepción de los preceptos legales, se trata de recomendaciones y por tal motivo su implementación como modelo es voluntario y por ello no se constituye como obligación de la Universidad acogerlos de manera integral, pero como estándar si considerarlos como base fundamental para el desarrollo del modelo de seguridad y privacidad de la información.

- Ley 1581 del 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1273 del 2009 articulo 269 numeral A al H, Ley que modifica el Código Penal; se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- ISO/IEC 27001: Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional actualizada en octubre de 2022 por la International Organization for Standardization (ISO) y por la International Electrotechnical Commission (IEC). Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información según el conocido “Ciclo de Deming”: denotado por las siglas PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

- Marco de ciberseguridad de la NIST: Es un conjunto de pautas para mitigar los riesgos de ciberseguridad organizacional, publicado por el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) basado en estándares, pautas y prácticas existentes. El marco proporciona una taxonomía de alto nivel de los resultados de la ciberseguridad y una metodología para evaluar y gestionar esos resultados, además de orientación sobre la protección de la privacidad y las libertades civiles en un contexto de ciberseguridad.

3.3 NORMAS DE LA POLITICA

- La autenticación de los usuarios para ingresar a la cuenta institucional, tendrá una verificación en dos pasos, adicional a la contraseña.
- Las contraseñas son de uso personal e intransferible y por ningún motivo se deberán prestar a otro usuario.
- La contraseña debe estar compuesta por una combinación de letras Mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /.
- Evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" ó "98765")
- No repetir los mismos caracteres en la misma contraseña. (ej.: "111222").
- No enviar nunca la contraseña por correo electrónico o en un sms, tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
- No deben usarse palabras o nombres comunes que aparezcan en los diccionarios.
- No debe haber una relación obvia con el usuario, sus familiares, nombre de la entidad, abreviaciones relacionadas a la entidad, ciudad, país, año, fecha de nacimiento, el grupo de trabajo u otras asociaciones parecidas, ya que pueden ser identificadas de manera fácil a través de un ataque de ingeniería social.
- Debe ser cambiada con una periodicidad de mínima de 60 días.
- Si hay indicios para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
- No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.
- No se debe almacenar la contraseña en la computadora. Algunos cuadros de diálogo o ventanas emergentes de los navegadores presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.
- No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a

usar contraseñas anteriores, esto se debe gestionar desde el sistema que asigne las credenciales.

4. ANEXOS

No aplica.