Diagonal 47 # 77B- 09 Int. 5 | Bogotá – Colombia
(+57- 1) - 746 6775 | andinoscontigo@andicoor.com.co
www.andicoor.com.co

NIT: 860.050.097-8 | **Código DIAN:** 0128

Andinos
AGENCIA DE ADUANAS NIVEL 1

Bogotá., 17 de Agosto de 2021

Política de confidencialidad

1. Propósito

El propósito de este documento es definir la política de confidencialidad informática Institucional con respecto al uso responsable de los sistemas de información. Se entiende por uso responsable el seguimiento de normas, políticas y buenas prácticas que salvaguarden la seguridad de los datos, sistemas de información y el buen uso de los recursos tecnológicos Institucionales.

Con el presente documento se establecen los controles para:

- ✓ Definir los responsables del manejo de la información.
- ✓ La creación, administración y asignación de roles.
- ✓ La administración de cuentas de acceso a los sistemas de información y correo electrónico.
- ✓ Politica creación de contraseñas.

2. Alcance

Esta política aplica para todos los **empleados** cualquiera sea su jerarquía, a los **contratistas**, y a cualquier otra persona que tenga acceso a los sistemas de información de la organización. Entendiendase por sistema de informacion el compendio de software, hardware y datos.

3. Responsables del manejo de la información

Cada usuario es responsable de almacenar la información en https://andicoorcol.sharepoint.com, plataforma asignada para el manejo de información en general de la organización.

Cada cuenta de usuario esta configurada para almacenar los datos generados por los aplicativos organizacionales; toda información guardada en otras ubicaciones del equipo no tendrá respaldo.

La unidad administrativa es la responsable de cumplir y hacer cumplir las políticas y procedimientos establecidos por la organización en el presente documento; asi como garantizar que la información este salvaguardada y disponible a traves de sistemas de backup licenciados y seguros.

4. Creación, administración y asignación de roles

De acuerdo con los niveles de cargo establecidos en la estructura organizacional se determinan los roles para el acceso a los sistemas de información en cada perfil de cargo. Teniendo en cuenta esta determinación el responsable de tecnología parametriza las herramientas digitales aplicables con el fin de otorgar los permisos y restricciones a cada usuario.

5. Administración de cuentas de acceso a los sistemas de información y correo electrónico

5.1. Condiciones generales

La contraseña es un código único, personal e intransferible, que no debe ser divulgado o compartido con terceras personas, el no observar esta buena práctica constituye una violación a las políticas de seguridad de la empresa.

Un usuario registrado y autorizado en la empresa, se debe autenticar siempre con su contraseña personal para acceder a los Sistemas de Información y a los servicios de la plataforma tecnológica.

Toda cuenta de usuario de la plataforma tecnológica debe identificar una persona en la vida real, empleado, no se permite el uso de cuentas genéricas o anónimas.

En caso de requerirse el acceso a la cuenta de un empleado que se encuentre fuera de las instalaciones de la empresa, únicamente el jefe inmediato o superior realizará la solicitud escrita a la Unidad Administrativa y esta autorizará para asignar una contraseña temporal con una duración específica, y luego la cuenta será desactivada; el solicitante será responsable de lo que suceda con los archivos de información y la seguridad por la duración del evento. Una vez el empleado retorne a las oficinas deberá ser informado del cambio de contraseña y solicitará la activación de su cuenta actualizando su contraseña manteniendo la confidencialidad de la misma.

El usuario es el responsable de garantizar la seguridad de la información a su cargo, la cual está disponible en medios electrónicos, utilizando para ello en todo momento las mejores prácticas de manejo documental, contraseñas seguras y dándole a esta el uso adecuado.

Las contraseñas tendrán un periodo de vigencia de CUARENTA Y CINCO (45) días, fecha en la cual se obligará a cambiarse de acuerdo con las mejores prácticas y políticas de seguridad, de lo contrario se desactiva la cuenta.

Es importante precisar que el usuario y la contraseña, es el mecanismo de identificación de un usuario ante la Empresa para el uso de los recursos tecnológicos y de información, esta identificación, permite manejar los perfiles y permisos de los usuarios, hacer el seguimiento y trazabilidad en caso de problemas de acceso y seguridad.

Únicamente las contraseñas de administración de la plataforma tecnológica deberán ser escritas, protegidas en un sobre debidamente sellado y almacenadas en un lugar seguro, con los datos del remitente, la fecha y el sistema, para ser utilizados en caso de una contingencia o de ausencia del líder del proceso.

5.2 Politica creacion de contraseñas

5.2.1 Contraseña Segura o fuerte:

Una contraseña segura, es un código especial para proteger sus recursos informáticos, debe contener letras mayúsculas y minúsculas, con números y caracteres especiales sin espacios, y tiene come finalidad disminuir la posibilidad de acceso no autorizado y que sea utilizada por un tercero, para suplantarnos ante la organización ocasionando fraude o falsificación.

Para esto se deben observar ciertas recomendaciones al momento de su creación, como por ejemplo no utilizar datos personales, tales como nombres, números de identificación, fechas que puedan ser utilizados por terceros para adivinar nuestra contraseña. Por ejemplo: compartiría la contraseña de su tarjeta débito o crédito, con un extraño? Claro que no, esto podría ocasionarle graves inconvenientes financieros; lo mismo ocurre con los activos tecnológicos, de nuestra Empresa.

Reglas para crear contraseñas fuertes, y así evitar el uso de su identidad por parte de personal no autorizado (suplantación):

- ✓ Elija contraseñas largas, de por lo menos 7 caracteres de longitud, o más
- ✓ Utilice dos números en los primeros siete caracteres.
- ✓ Dentro de su contraseña no utilice un nombre, una cadena de números, ni ninguna palabra común que aparezca en un diccionario.
- ✓ Utilizar mayúsculas y minúsculas intercaladas dentro de los 7 caracteres.
- ✓ Algunos caracteres especiales pueden ser utilizados; sin embargo, tenga en cuenta que algunas aplicaciones no pueden aceptar caracteres especiales.
- ✓ Uno de los métodos de generación de contraseñas más fáciles de recordar y más difíciles de violar es el de contraseña pseudo-aleatoria. En este caso, la contraseña se genera a partir de una frase fácil de recordar que es importante para el usuario. Esta puede ser una frase de un libro que le gusta en especial, las palabras de una canción que siempre recuerde con facilidad, una frase que usted nunca olvidará.

5.2.2. Evitar contraseñas debiles:

Al crear contraseñas, evitar el texto siguiente:

- ✓ Contraseñas fáciles de adivinar, como contraseñas en blanco o palabras como “contraseña”, “amor”, “super”, etc.
- ✓ Su nombre, nombre del cónyuge o de su hijo.
- ✓ El nombre de su mascota.
- ✓ Nombres de amigos cercanos o compañeros de trabajo.
- ✓ Nombres de sus personajes favoritos de fantasía.
- ✓ El nombre de su jefe.
- ✓ El nombre, en general, de alguien.
- ✓ Cadenas de números o letras, al igual que 1234, abcde.
- ✓ El nombre de su equipo.
- ✓ Su número de teléfono o su número de placa
- ✓ Cualquier parte de sus documentos de identificación
- ✓ Una fecha de nacimiento
- ✓ Otros información suya que sea fácil de obtener (por ejemplo, dirección, ciudad, oficina)
- ✓ Una palabra en un diccionario de cualquier idioma
- ✓ Nombres de lugares o nombres propios
- ✓ Las contraseñas con una sola letra repetida como ’aaaa’
- ✓ Patrones simples de letras en el teclado, como asdf
- ✓ Todo lo anterior escrito hacia atrás
- ✓ Cualquiera de las anteriores seguida o precedida de un solo dígito (número)

5.2.3.Caracteres especiales no permitidos

Carácteres excluidos de la lista de carácteres especiales por ser incompatibles con algunos sistemas:

- ✓ Espacio
- ✓ "Comilla Doble"
- ✓ 'Comilla simple'
- ✓ `Backtick`
- ✓ & Ampersand: &
- ✓ Paréntesis (izquierdo o derecho ( )
- ✓ | Barra |
- ✓ < Inferior a <
- ✓ Superior a >

Las claves iniciales de ERP son controlados por el Strategic Controller y actualizadas por el usuario de manera programada por el sistema.

Diagonal 47 # 77B- 09 Int. 5 | Bogotá – Colombia
(+57- 1) - 746 6775 | andinoscontigo@andicoor.com.co
www.andicoor.com.co

NIT: 860.050.097-8 | **Código DIAN:** 0128

Andinos
AGENCIA DE ADUANAS NIVEL 1

Los sistemas de información y cuentas de sistema operativo solicitarán automáticamente el cambio de las contraseñas cada 90 días, las de el ERP solicitará cambio cada 72 días.

Cuando ingresa un nuevo usuario se le asigna una clave genérica para su equipo y debe cambiarse el mismo día del ingreso. Para las claves de correo electrónico corporativo, tecnología se conecta remoto para asignarla.

6. Garantizar la confidencialidad de la información

Adicionalmente y con el fin de garantizar la confidencialidad de la información, la organización establece los siguientes controles que permitan mitigar el riesgo de filtracion o perdida de la misma:

Acuerdo de confidencialidad, y Acuerdo de seguridad bilateral; los cuales son firmados por el colaborador en el mismo momento de recibir la respectiva induccion de calidad y seguridad.

Cordialmente,

ORIGINAL FIRMADO

Juan Guillermo Díaz Castañeda
CC. 1.020.751.053
Representante Legal

Control de cambios.

Versión revisada	Descripción de la modificación o anulación *(incluya la fuente que origina el cambio)*	Versión vigente	Fecha de aprobación.	Fecha de vigencia.
N.A.	Establecimiento de la política de gestión en controlk de seguridad.	1	04/06/2021	04/02/2022
1	Se incluye el numeral 5.2 “Politica creación de contraseñas”.	2	19/07/2021	19/07/2022
2	Se reestructura la PolÍtica sepárandola en “Politica de confidencialidad” y “Politica de uso de recursos informáticos”.	3	17/08/2021	17/08/2022