Política de gestión de usuarios y contraseñas

1. Objetivo.

Definir las políticas de gestión de usuarios y contraseñas, con el objetivo de educar a los usuarios finales a hacer uso correcto de los sistemas y herramientas proporcionados por la empresa, así mismo, evitar la vulneración de los sistemas o pérdida de información debido a malas manipulaciones de credenciales de los usuarios.

2. Alcance.

Se extiende la presente política de gestión de usuarios y contraseñas a todas las áreas, departamentos, secciones o entidades de Fruno y son de cumplimiento obligatorio por parte de todos los funcionarios y empleados en cualquier nivel jerárquico, sean temporales o permanentes.

3. Responsables.

- **Jefatura de TI:** Corresponde también al administrador de seguridad informática – administrador de sistemas. Es responsable de la administración integral, de la disponibilidad, la seguridad y del correcto funcionamiento de los sistemas informáticos de Fruno. Además, se encarga de mantener actualizada esta política, garantizando su estricto cumplimiento de manera constante. En caso de detectar incumplimientos de la política, debe solicitar la corrección de manera inmediata. Si no se obtiene una respuesta positiva en un lapso mayor a 4 días por parte del usuario, es responsable de informar a las jefaturas y al Departamento de Recursos Humanos para iniciar un proceso disciplinario hacia el usuario que ha desobedecido la política establecida.

- **Departamento de TI:** Cumple la importante función de asistir a los usuarios en la preconfiguración de sus dispositivos informáticos, garantizando la seguridad mediante la instalación de aplicaciones de protección y la revisión minuciosa de las configuraciones. Además, lleva a cabo auditorías regulares para asegurar que los equipos estén debidamente resguardados y preparados para afrontar cualquier eventualidad que pueda comprometer la seguridad de la información.
- **Supervisor o Jefatura de departamento:** Es el responsable de velar por que cada usuario a su cargo cumpla con las políticas de seguridad adjuntas en el presente documento, tiene la obligación de reportar inmediatamente a la Jefatura de TI cualquier anomalía identificada, vía osticket, correo electrónico o llamada telefónica en caso de una emergencia, en caso de desatención de los lineamientos de esta política por parte de los colaboradores a su cargo es responsable de solicitar e iniciar un proceso disciplinario en coordinación con el Departamento de Recursos Humanos.
- **Usuario:** Es cualquier empleado de la empresa, sea temporal o permanente, que tenga acceso a sistemas de información o herramientas brindadas que requieran credenciales para poder acceder y que, sin importar el cargo o rol que cumpla dentro de la compañía, debe cumplir con cada punto estipulado en esta política.
- **Departamento de Recursos Humanos:** Es el departamento encargado de tomar acciones disciplinarias contra aquel usuario que no cumpla con lo establecido en esta política, y le sea reportado.

4. Documentos aplicables.

N/A

5. Definiciones.

Credenciales: Son la combinación de información que se utiliza para verificar la identidad de un usuario y permitirle el acceso a un sistema o servicio. Las

credenciales típicamente incluyen un nombre de usuario y una contraseña, aunque también pueden incluir otros elementos como certificados digitales o tokens de autenticación.

Usuario genérico: Se refiere a un usuario que no se identifica a una única persona y que suele ser compartido o empleado por diferentes trabajadores.

6. Desarrollo.

Política.

Gestión de Credenciales.

6.1. Los usuarios de los sistemas informáticos de la empresa tienen la obligación de establecer y mantener una contraseña robusta para los sistemas que utiliza, entre las características obligatorias de la contraseña es que debe estar compuesta por:

- Una longitud mayor o igual a 12 dígitos.
- Debe incluir al menos dos números diferentes.
- Debe contener letras minúsculas y mayúsculas.
- Debe contener al menos un carácter especial.

6.2. El usuario no debe aceptar recibir contraseñas por parte del Departamento de TI que no cumplan con las características estipuladas en el punto 6.1..

6.3. Esta estrictamente prohibido utilizar credenciales y contraseñas que no cumplan con esta política.

Prohibiciones.

6.4. Esta estrictamente prohibido:

6.4.1. Utilizar información personal como contraseña o como contenido de la misma, por ejemplo: Cédula, Nombre, edad, Fecha Nacimiento, Nombre de algún familiar.

6.4.2. Reutilizar contraseñas antiguas, ya que posiblemente estas puede que hayan sido comprometidas en alguna ocasión.

6.4.3. Utilizar la misma contraseña para diferentes sistemas. Es obligatorio que cada sistema cuente con su propia contraseña.

6.5. No se debe utilizar como contraseña o en parte de esta, patrones de teclado ni números en secuencia, por ejemplo 1234 – qwerty.

6.6. No se debe repetir caracteres, por ejemplo, aaaa,1111, qqqq en la contraseña.

6.7. Se prohíbe utilizar el nombre de la empresa o departamento al que pertenece en sus credenciales, en la contraseña.

6.8. Esta estrictamente prohibido compartir sus credenciales con otros usuarios. Está prohibido ceder o prestar las credenciales asignadas por el administrador de sistemas, el usuario debe proteger meticulosamente sus credenciales, evitando que sean robadas o vulnerables.

6.9. Se prohíbe ingresar a sistemas con usuarios genéricos no identificados o usuarios que no le pertenecen, salvo los que sí han sido compartidos y autorizados por el departamento de TI (algunos ejemplos corresponde a aquellos designados para una máquina o equipo en específico que no se asocian con un único usuario, como las computadoras para realizar traslados en el área de bodega, usuarios asignados a un punto de venta en el área comercial, usuarios asignadas a máquinas de carga de software o IMEI en taller, otros). Está estrictamente prohibido realizar transacciones en cualquiera de los sistemas de Fruno con credenciales de otros usuarios y que no han sido asignados por el administrador del sistema.

6.10. Está prohibido tener expuesta la contraseña en su lugar de trabajo por medio de “posticks”, o “papelitos” que comprometan la confidencialidad de sus credenciales. Se prohíbe al usuario guardar su contraseña en una forma legible en archivos en disco; tampoco debe escribirla en papel, dejarla en sitios donde pueda ser encontrada o compartirla o revelarla a cualquier otra persona. El usuario que viole esta normativa será responsable directo por todos los daños y perjuicios que resulten de tal violación.

6.11. Se prohíbe la utilización de códigos QR como “enmascaramiento” de contraseñas que permitan el ingreso a cualquier sistema de la organización.

6.12. Se prohíbe utilizar las mismas credenciales de la empresa en sus redes sociales o herramientas personales externas.

6.13. Se prohíbe ingresar a los sistemas o herramientas de le empresa fuera de horario laboral sin previa autorización escrita de su Jefatura directa, estos accesos deben ser reportados al Departamento de TI para que no sean bloqueados y tipificados como accesos no identificados.

6.14. Se prohíbe conectarse a los sistemas de la empresa desde lugares públicos o redes inalámbricas compartidas, como lo son las redes de los restaurantes, parques, centros comerciales, universidades o cualquier otro sitio donde las redes se encuentren expuestas o públicas para cualquier tipo de usuario.

Cambio de Contraseñas.

6.15. Como medida de seguridad, todos los usuarios finales deben realizar el cambio de contraseña cada 90 días, deben solicitar por medio de un ticket o vía correo electrónica el cambio de contraseñas al Departamento de TI, esto en caso de que el sistema no permita autogestionarse las credenciales.

6.16. Es importante que el usuario tenga claro que puede realizar el cambio de sus credenciales cuando así lo requiera, más si considera que sus credenciales actuales se encuentran en riesgo o fueron expuestas a un tercero. Es responsabilidad del usuario cambiar inmediatamente su contraseña cuando tenga indicio o razón suficiente para creer que ha sido comprometida, o de acuerdo a la política establecida por Fruno (cada 90 días calendarios).

6.17. Prohibido utilizar contraseñas que sean idénticas o sustancialmente similares a contraseñas previamente empleadas. Es requerido que cada vez que se actualice una contraseña la misma no haya sido reciclada ni utilizada en ningún otro sistema.

Otras Obligaciones.

6.18. Cada usuario es responsable de reportar a su Jefatura inmediata cualquier situación que ponga en riesgo la seguridad de sus credenciales.

6.19. El usuario final debe reportar la pérdida o robo de sus credenciales de manera inmediata a su Jefatura directa, para que este seguidamente y con la urgencia del caso lo reporte a la Jefatura de TI.

6.20. El usuario final debe reportar inmediatamente cualquier cambio en los sistemas registrados con su usuario que considere que nunca realizó.

6.21. Por ningún motivo el usuario debe dejar sistemas abiertos o el equipo de trabajo desbloqueado cuando se encuentre ausente de su lugar de trabajo.

6.22. Es importante considerar que, se limita a tres (3) el número consecutivo de intentos infructuosos para introducir la contraseña de usuario; después del tercero y último intento la cuenta involucrada queda bloqueada y se deberá notificar al departamento de informática, para que se genera una nueva contraseña y procedan con el desbloqueo.

6.23. El incumplimiento de la presente política dará lugar a la aplicación de las sanciones laborales establecidas de conformidad al Código de Trabajo, el Reglamento Interno de Trabajo de Fruno y demás disposiciones internas relacionadas, sin perjuicio de las acciones civiles o penales que, en su caso, puedan resultar aplicables.

Control de versiones:

Número	Nombre	Revisiones	Fecha
1	Junior Sánchez Bolaños	Rev A. Creación del documento	10/02/2023
2	Junior Sánchez Bolaños	Rev B. Cambios de redacción en el documento, eliminación de sesiones que pertenecen más a un procedimiento que a una política	08/05/2024
3			
4			
5			
6			
7			
8			
9			
10			