**2 Proceso de Verificación de Usuario**

**Verificación de Usuario**

1. **Inicio: Usuario inicia la aplicación o sistema.**
   * **(Forma de entrada: Cuadro de Inicio)**
2. **Pantalla de Login: Usuario ingresa sus credenciales (usuario y contraseña).**
   * **(Forma de entrada: Cuadro de acción)**
3. **Validación de Entrada:**
   * **Si los campos de usuario o contraseña están vacíos, mostrar mensaje de error y redirigir al paso 2.**
   * **(Forma de decisión: Cuadro de decisión con dos ramas: "Completo" o "Error")**
4. **Verificación de Credenciales en la Base de Datos:**
   * **Si el usuario y contraseña son correctos, procede al siguiente paso.**
   * **Si son incorrectos, mostrar mensaje de error e incrementar el contador de intentos fallidos.**
   * **(Forma de decisión con dos ramas: "Correcto" o "Incorrecto")**
5. **Verificación de Número de Intentos:**
   * **Si los intentos fallidos superan el límite permitido, bloquear cuenta temporalmente y enviar notificación al usuario.**
   * **(Forma de decisión: "Intentos Excedidos" o "Intentos Permitidos")**
6. **Verificación de Autenticación de Dos Factores (si está habilitado):**
   * **Enviar código al usuario (correo/SMS/app de autenticación).**
   * **Usuario ingresa el código recibido.**
   * **(Forma de entrada y acción adicional)**
7. **Validación del Código:**
   * **Si el código es correcto, procede al acceso.**
   * **Si es incorrecto, redirigir al paso de verificación.**
   * **(Forma de decisión con dos ramas: "Correcto" o "Incorrecto")**
8. **Acceso al Sistema: Permitir al usuario acceder al sistema y redirigirlo a la pantalla principal.**
   * **(Forma de acción)**
9. **Fin**

**Diagrama

Descripción generada automáticamente**

**Objetivo**

**El objetivo del proceso de verificación de usuario es confirmar la identidad del usuario para garantizar la seguridad y la integridad del sistema o aplicación. Este proceso tiene como propósito principal:**

1. **Proteger la información y los recursos del sistema al evitar accesos no autorizados, asegurando que solo los usuarios legítimos puedan interactuar con datos sensibles o realizar acciones específicas.**
2. **Prevenir el fraude y el uso indebido de cuentas mediante mecanismos que validen la identidad del usuario, tales como contraseñas, autenticación de múltiples factores, biometría, entre otros.**
3. **Mejorar la confianza del usuario en la plataforma, proporcionando medidas de seguridad que protejan su información y garanticen una experiencia de uso segura.**

**Este proceso contribuye al fortalecimiento de la ciberseguridad en el sistema y al cumplimiento de las normativas de protección de datos, creando un entorno de interacción confiable para los usuarios.**

**Frecuencia**

**La frecuencia del proceso de verificación de usuario puede variar según la sensibilidad de los datos, la política de seguridad del sistema y el nivel de acceso requerido. Las opciones comunes incluyen:**

1. **Inicio de sesión: Cada vez que el usuario accede al sistema o aplicación.**
2. **Sesiones sensibles: Antes de realizar operaciones de alto riesgo, como cambios en la configuración, transferencias de datos sensibles o transacciones financieras.**
3. **Períodos regulares: Re-verificación cada cierto tiempo, como cada 24 horas, al final de una sesión prolongada o al detectar inactividad, para reforzar la autenticación continua.**
4. **Cambios en el dispositivo o ubicación: Verificación adicional si el usuario accede desde un dispositivo o ubicación nueva, a fin de asegurar la autenticidad del acceso.**

**Implementar una frecuencia de verificación adecuada ayuda a mantener un equilibrio entre la seguridad y la experiencia de usuario.**

**Documentos de Entrada**

**Credenciales del usuario:**

* **Nombre de usuario: Identificación única del usuario en el sistema.**
* **Contraseña: Se utiliza para autenticar la identidad del usuario. Debe ser almacenada de manera segura.**

**Métodos de autenticación:**

* **Tokens de autenticación: Generados por aplicaciones de autenticación o enviados a través de SMS o correo electrónico para la verificación de dos pasos (2FA).**
* **Datos biométricos: Huellas dactilares, reconocimiento facial o escaneo de iris, si se utiliza autenticación biométrica.**

**Registro de actividad del usuario:**

* **Historial de inicios de sesión: Información sobre los últimos accesos, incluidos horarios, dispositivos utilizados y ubicaciones.**
* **Datos de sesión: Información relacionada con la sesión actual, como la duración y el estado de la conexión.**

**Políticas de seguridad y autenticación:**

* **Normativas internas: Documentación que define los requisitos de seguridad, como complejidad de contraseñas y reglas para la autenticación de múltiples factores.**
* **Protocolos de acceso: Reglas específicas sobre cuándo y cómo se debe realizar la verificación del usuario.**

**Sistema de gestión de identidades:**

* **Base de datos de usuarios: Contiene información de los usuarios, sus roles y permisos en el sistema.**

**Alertas y eventos de seguridad:**

* **Incidencias de seguridad previas: Información sobre intentos fallidos de inicio de sesión o accesos no autorizados que pueden requerir una verificación más estricta.**

**Documentos de Salida**

**Informe de autenticación:**

* **Detalles sobre el éxito o fracaso del proceso de verificación, incluyendo la hora, el método de autenticación utilizado y el resultado final (autenticación exitosa o fallida).**

**Registro de acceso del usuario:**

* **Un registro que documenta cada acceso del usuario, incluyendo:**
  + **Fecha y hora del acceso.**
  + **Dirección IP desde la cual se realizó el acceso.**
  + **Dispositivo utilizado (si es aplicable).**
  + **Ubicación geográfica (si se está utilizando la geolocalización).**

**Alertas y notificaciones:**

* **Alertas de acceso no autorizado: Notificaciones enviadas al usuario o al equipo de seguridad si se detecta un intento de acceso no autorizado.**
* **Notificaciones de cambios de credenciales: Informes sobre la actualización de contraseñas o cambios en la configuración de seguridad.**

**Tokens de sesión:**

* **Tokens o identificadores únicos generados para la sesión del usuario, que permiten el acceso durante un periodo determinado sin necesidad de volver a autenticar.**

**Datos de actividad del usuario:**

* **Información sobre las acciones realizadas durante la sesión, que puede ser utilizada para auditorías o análisis de comportamiento.**

**Informe de auditoría de seguridad:**

* **Un resumen que incluye estadísticas sobre intentos de acceso, número de accesos exitosos y fallidos, así como patrones que podrían indicar intentos de fraude o brechas de seguridad.**

**Estado de la cuenta:**

* **Información sobre el estado de la cuenta del usuario, indicando si está activa, inactiva, bloqueada o si requiere atención adicional (por ejemplo, restablecimiento de contraseña).**

**Area responsable**

**Departamento de Tecnología de la Información (TI):**

* **Responsabilidad: Implementar y mantener los sistemas de autenticación y control de acceso. Se encargan de la infraestructura técnica que soporta el proceso de verificación de usuario, incluyendo servidores, bases de datos y protocolos de seguridad.**

**Equipo de Seguridad Informática:**

* **Responsabilidad: Supervisar la seguridad de la información y proteger los datos de acceso. Están encargados de definir las políticas de seguridad, realizar auditorías, monitorear accesos y responder a incidentes de seguridad.**

**Soporte Técnico:**

* **Responsabilidad: Asistir a los usuarios en caso de problemas relacionados con la verificación de su identidad, como olvidos de contraseña o bloqueos de cuenta.**

**Política de Operaciones para el Proceso de Verificación de Usuario**

**Objetivo de la Política:Proteger la integridad y confidencialidad de los datos de acceso mediante un proceso de verificación de usuario robusto y seguro.**

**Alcance:Esta política se aplica a todos los empleados, contratistas y terceros que acceden a los sistemas de información de la organización.**

**Requisitos de Autenticación:**

* + **Contraseñas: Las contraseñas deben tener una longitud mínima (por ejemplo, 8-12 caracteres) y cumplir con criterios de complejidad (incluir letras mayúsculas, minúsculas, números y caracteres especiales).**
  + **Autenticación de Múltiples Factores (MFA): Se debe implementar MFA para todos los accesos que involucren información sensible o sistemas críticos.**

**Procedimientos de Verificación:**

* + **Inicio de Sesión: Los usuarios deberán ingresar su nombre de usuario y contraseña, seguidos de un segundo factor de autenticación si se requiere MFA.**
  + **Sesiones Inactivas: Las sesiones deben cerrarse automáticamente tras un período de inactividad (por ejemplo, 15-30 minutos).**
  + **Acceso desde Nuevos Dispositivos o Ubicaciones: Se debe realizar una verificación adicional cuando un usuario intenta acceder desde un dispositivo o ubicación desconocida.**

**Gestión de Credenciales:**

* + **Restablecimiento de Contraseña: Los procedimientos para restablecer contraseñas deben requerir verificación adicional, como preguntas de seguridad o códigos enviados a correos electrónicos/telefonos registrados.**
  + **Bloqueo de Cuenta: Las cuentas deben bloquearse después de un número determinado de intentos fallidos de inicio de sesión (por ejemplo, 3-5 intentos) y requerir intervención del soporte técnico para su desbloqueo.**

**Monitoreo y Registro:**

* + **Todos los intentos de inicio de sesión, tanto exitosos como fallidos, deben ser registrados y monitoreados para detectar actividades sospechosas.**
  + **Se deben realizar auditorías regulares de los registros de acceso para identificar patrones inusuales.**

**Entrenamiento y Concienciación:**

* + **Se debe proporcionar formación regular a los empleados sobre las mejores prácticas de seguridad, la importancia de la verificación de usuario y cómo manejar sus credenciales de manera segura.**

**Revisión y Actualización de la Política:**

* + **La política debe revisarse al menos anualmente o después de cualquier incidente de seguridad significativo para asegurarse de que sigue siendo efectiva y relevante.**

**Consecuencias del Incumplimiento:**

* + **Se establecerán consecuencias para aquellos que no cumplan con esta política, que pueden incluir medidas disciplinarias y revocación de acceso a sistemas.**