TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

GESTION DE ACCESOS

Actividad # 1

Balbuena Atar Dante Gabriel

Tafí viejo Tucumán Argentina – 2025/05/04

Profesor: Marcelo Daniel Rossetti

Contenido

1. Introducción

El proceso de recuperación de contraseña es un componente fundamental en la gestión segura de identidades dentro de cualquier sistema informático. Su correcta implementación garantiza que los usuarios puedan restablecer el acceso a sus cuentas de manera confiable, sin comprometer la seguridad de la información. Este documento detalla las etapas que componen dicho proceso, los componentes tecnológicos involucrados y los controles necesarios para asegurar su eficacia, todo enmarcado en buenas prácticas alineadas con estándares internacionales como ISO 27001 y marcos de referencia como COBIT.

2. Desarrollo

Proceso de Recuperación de Contraseña

1.1. Diagrama de Flujo del Proceso

1.2 Descripción de Etapas

Solicitud de recuperación:

El usuario indica que olvidó su contraseña o su cuenta está bloqueada por intentos fallidos.

Validación de identidad:

El sistema verifica al usuario mediante métodos predefinidos (correo alternativo, OTP, preguntas de seguridad).

Envío de enlace/código:

Se envía un enlace temporal o código de un solo uso (OTP) al método de contacto registrado (correo/SMS).

Ingreso de código/enlace:

El usuario introduce el código o accede al enlace para confirmar su identidad.

Creación de nueva contraseña:

El usuario define una nueva contraseña que cumple con las políticas de seguridad (ej: longitud, caracteres especiales).

Actualización y notificación:

El sistema actualiza la contraseña y notifica al usuario del cambio.

Registro de actividad:

Se guarda un log de la operación para auditoría.

1.3 Componentes de TI Involucrados

Servidor de autenticación: Gestiona las credenciales y el proceso de recuperación (ej: Active Directory, LDAP).

Base de datos de usuarios: Almacena información de cuentas y métodos de recuperación.

Sistema de correo electrónico/SMS: Envía códigos o enlaces temporales.

Aplicación web/móvil: Interfaz donde el usuario inicia la recuperación.

Herramientas de logging: Registran intentos de recuperación y cambios de contraseña (ej: SIEM).

Firewall/IPS: Protege contra ataques de fuerza bruta o phishing.

1.4 Controles a Aplicar

Controles de autenticación:

Uso de autenticación multifactor (OTP, correo de verificación).

Preguntas de seguridad personalizadas (no basadas en información pública).

Controles de seguridad:

Encriptación de comunicaciones (HTTPS, TLS).

Limitación de intentos fallidos para evitar ataques de fuerza bruta.

Caducidad rápida de enlaces/códigos temporales (ej: 15 minutos).

Controles de contraseña:

Política de complejidad (mínimo 12 caracteres, mayúsculas, números).

Prohibición de reutilizar contraseñas anteriores.

Controles de auditoría:

Registro detallado de actividades (logs de acceso, cambios de contraseña).

Alertas por actividades sospechosas (ej: múltiples recuperaciones desde una IP desconocida).

Controles organizativos:

Capacitación a usuarios sobre phishing y seguridad de contraseñas.

Revisión periódica de políticas de recuperación (alineado con ISO 27001 o COBIT).

3. Conclusiones

La recuperación de contraseñas no solo debe centrarse en la facilidad para el usuario, sino también en establecer mecanismos de control robustos que minimicen riesgos de suplantación de identidad o accesos no autorizados. La implementación de múltiples capas de seguridad, la auditoría constante y la capacitación del usuario son pilares esenciales para garantizar un proceso confiable y alineado con las exigencias actuales en ciberseguridad. Un enfoque integral permite a las organizaciones mantener la continuidad operativa sin descuidar la protección de los activos digitales.