

**Políticas de seguridad**

### **1. Política de Control de Acceso**

**Objetivo**: Asegurar que sólo los usuarios autorizados tengan acceso a los recursos del sistema y las funciones relacionadas con la cobranza.

* **Autenticación multifactor (MFA)**: Implementar autenticación en dos pasos para todos los usuarios que accedan a datos sensibles o funciones críticas.
* **Roles y permisos**: Definir roles de usuario claros (por ejemplo, administrador, cobrador, supervisor) con permisos específicos para cada uno, limitando el acceso a información y funciones según el rol.
* **Revisión periódica de permisos**: Realizar auditorías regulares para revisar los permisos de los usuarios y asegurarse de que los accesos estén alineados con las responsabilidades actuales de los empleados.

### **2. Política de Gestión de Contraseñas**

**Objetivo**: Asegurar que las contraseñas utilizadas por los usuarios sean robustas y seguras.

* **Requisitos de contraseñas fuertes**: Establecer reglas de complejidad de contraseñas (longitud mínima, uso de caracteres especiales, números, mayúsculas y minúsculas).
* **Caducidad de contraseñas**: Implementar un ciclo de renovación de contraseñas cada 60-90 días.
* **Almacenamiento seguro de contraseñas**: Asegurarse de que todas las contraseñas se almacenen encriptadas utilizando algoritmos de hash seguros (como bcrypt).
* **Bloqueo por intentos fallidos**: Bloquear las cuentas después de un número determinado de intentos fallidos de inicio de sesión y exigir verificaciones adicionales para desbloquearlas.

### **3. Política de Protección de Datos**

**Objetivo**: Proteger la confidencialidad e integridad de los datos sensibles manejados por la plataforma, como la información personal y financiera de los clientes.

* **Cifrado de datos en tránsito y en reposo**: Implementar cifrado SSL/TLS para proteger la información durante la transmisión. Además, todos los datos almacenados deben estar cifrados (AES-256, por ejemplo).
* **Minimización de datos**: Limitar la recopilación de datos personales únicamente a los necesarios para la operación del servicio.
* **Acceso limitado a datos sensibles**: Los datos personales y financieros sólo deben ser accesibles para los empleados que los necesiten para realizar su trabajo.
* **Política de retención de datos**: Definir períodos de retención para los datos almacenados y procedimientos para eliminar los datos cuando ya no sean necesarios.

### **4. Política de Gestión de Vulnerabilidades**

**Objetivo**: Identificar y corregir vulnerabilidades de seguridad de manera proactiva.

* **Análisis de vulnerabilidades periódicos**: Realizar escaneos de vulnerabilidades de manera regular en toda la plataforma, identificando posibles brechas.
* **Actualizaciones de software y parches**: Establecer procedimientos para aplicar actualizaciones y parches de seguridad tan pronto como estén disponibles, tanto en los sistemas operativos como en las aplicaciones y bases de datos.
* **Pruebas de penetración**: Llevar a cabo pruebas de penetración periódicas para identificar debilidades que no puedan ser detectadas por escaneos automáticos.
* **Divulgación responsable de vulnerabilidades**: Establecer un canal donde los usuarios y terceros puedan reportar de manera segura posibles vulnerabilidades.

### **5. Política de Respuesta a Incidentes**

**Objetivo**: Establecer un proceso formal para responder eficazmente a incidentes de seguridad, minimizando el impacto en la operación.

* **Plan de respuesta a incidentes**: Crear un plan formal de respuesta a incidentes que detalle los pasos a seguir en caso de una violación de seguridad, incluyendo asignación de responsabilidades, comunicación y remediación.
* **Monitoreo continuo**: Implementar sistemas de monitoreo en tiempo real que identifiquen comportamientos inusuales y alerten al equipo de seguridad.
* **Registro y auditoría de eventos**: Registrar todas las actividades críticas (como inicios de sesión, cambios en los datos, intentos de acceso no autorizados) para realizar auditorías y detectar posibles incidentes de seguridad.
* **Notificación de violaciones de datos**: Establecer un protocolo de notificación inmediata a los clientes y reguladores en caso de violación de datos.

### **6. Política de Seguridad de la Red**

**Objetivo**: Proteger la infraestructura de red de la plataforma contra ataques externos y accesos no autorizados.

* **Firewalls y sistemas de detección de intrusiones (IDS/IPS)**: Implementar firewalls avanzados y sistemas de detección/prevención de intrusiones para filtrar tráfico malicioso.
* **Segmentación de redes**: Separar las redes internas de las externas y crear zonas seguras para los datos más sensibles (como los sistemas de bases de datos).
* **VPN y conexiones seguras**: Requerir que todo el acceso remoto a la red de Alloxentric se realice a través de redes privadas virtuales (VPN) y conexiones cifradas.
* **Revisión de configuración de red**: Realizar auditorías regulares de la configuración de la red para detectar posibles puntos débiles.

### **7. Política de Continuidad de Negocio y Recuperación ante Desastres**

**Objetivo**: Asegurar que el servicio de optimización de cobranza de Alloxentric pueda continuar operando o recuperarse rápidamente en caso de fallos graves o desastres.

* **Copias de seguridad periódicas**: Implementar backups regulares de todos los datos críticos, almacenados en ubicaciones seguras y con capacidad de restauración rápida.
* **Plan de recuperación ante desastres (DRP)**: Desarrollar un plan formal para recuperar las operaciones tras desastres o incidentes importantes, detallando los procedimientos de restauración de sistemas y datos.
* **Pruebas de continuidad**: Realizar simulaciones regulares para probar la eficacia del plan de recuperación ante desastres y asegurar que el personal esté familiarizado con sus responsabilidades.

### **8. Política de Educación y Concienciación en Seguridad**

**Objetivo**: Asegurar que todos los empleados y usuarios estén formados en las mejores prácticas de seguridad y sean conscientes de los riesgos.

* **Capacitación regular en seguridad**: Proporcionar formación continua a los empleados sobre buenas prácticas de seguridad, como el reconocimiento de intentos de phishing y el manejo seguro de datos.
* **Concienciación sobre riesgos**: Mantener a los empleados informados sobre nuevas amenazas y tendencias de seguridad que puedan afectar a la plataforma.
* **Política de cumplimiento**: Establecer sanciones para aquellos empleados que violen las políticas de seguridad o pongan en riesgo la plataforma.

### **9. Política de Auditoría y Cumplimiento**

**Objetivo**: Garantizar el cumplimiento de las normativas de seguridad aplicables y de las mejores prácticas de la industria.

* **Auditorías periódicas**: Realizar auditorías internas y externas de seguridad de manera regular para verificar el cumplimiento con las normativas de seguridad aplicables (por ejemplo, GDPR, PCI-DSS).
* **Conformidad regulatoria**: Mantenerse actualizado con los requisitos legales y de cumplimiento en materia de protección de datos y seguridad en los países donde opera Alloxentric.
* **Mejora continua**: Establecer un proceso de revisión y mejora continua de las políticas de seguridad, basándose en los resultados de auditorías y en la evolución de las amenazas.

Estas políticas proporcionarán una base sólida para proteger los datos y la infraestructura de Alloxentric, asegurando el cumplimiento normativo y la protección contra amenazas de seguridad que puedan poner en riesgo el sistema de optimización de cobranza.