Política de Contraseñas Seguras

1. Propósito
El propósito de esta política es establecer los requisitos de seguridad para la creación, mantenimiento y gestión de contraseñas dentro de la empresa, con el objetivo de proteger los sistemas de información críticos y garantizar la confidencialidad, integridad y disponibilidad de los datos.

2. Alcance
Esta política se aplica a todos los empleados, contratistas y terceros que tengan acceso a sistemas informáticos y recursos de información dentro de la empresa. Esto incluye acceso a plataformas como sistemas ERP, bases de datos, correo electrónico corporativo, redes internas y otras herramientas críticas.

3. Requisitos de Contraseñas
Las contraseñas deben cumplir con los siguientes requisitos:

- **Longitud Mínima**: Las contraseñas deben tener una longitud mínima de 12 caracteres.
- **Complejidad**: Las contraseñas deben contener al menos:
    - Una letra mayúscula.
    - Una letra minúscula.
    - Un número.
    - Un carácter especial (como !, @, #, etc.).
- **No Reutilización de Contraseñas**: Las contraseñas no deben ser reutilizadas entre diferentes sistemas o servicios.
- **Prohibición de Contraseñas Comunes**: No se permitirán contraseñas comunes o fáciles de adivinar, como "123456", "password", o similares.
- **Cambio Periódico de Contraseñas**: Las contraseñas deben ser cambiadas cada 90 días como máximo. Las contraseñas anteriores no pueden ser reutilizadas en los siguientes tres cambios.
- **Bloqueo de Cuenta**: Después de 5 intentos fallidos de acceso, la cuenta será bloqueada temporalmente durante un período de 15 minutos.
- **Autenticación Multifactor (MFA)**: Para accesos a sistemas críticos, se debe habilitar la autenticación multifactor (MFA), como una capa adicional de seguridad.

4. Gestión de Contraseñas
Los usuarios deberán utilizar **administradores de contraseñas** aprobados por la empresa para almacenar y gestionar contraseñas de manera segura. Está prohibido escribir contraseñas en lugares no seguros (como notas físicas o archivos no cifrados).

5. Revisión y Auditoría

- **Auditoría Regular**: Se realizarán auditorías periódicas para asegurar el cumplimiento de esta política. Las contraseñas que no cumplan con los requisitos de seguridad establecidos serán deshabilitadas y los usuarios deberán cambiarlas.
- **Revisión de Accesos**: Se llevará a cabo una revisión periódica de los accesos de los usuarios a los sistemas y recursos críticos, especialmente cuando haya cambios de rol o salida de personal.

6. Responsabilidades

- **Responsabilidad del Usuario**: Cada usuario es responsable de mantener la confidencialidad de sus contraseñas y de seguir esta política de manera rigurosa.
- **Responsabilidad del Administrador de Sistemas**: Los administradores de sistemas son responsables de la implementación técnica de los requisitos de contraseñas en los sistemas, así como de la configuración y gestión de los bloqueos de cuentas y autenticación multifactor.

7. Excepciones
Cualquier solicitud de excepción a esta política debe ser solicitada por escrito a la Dirección de TI y será evaluada según los riesgos y necesidades de seguridad.

8. Sanciones
El incumplimiento de esta política puede resultar en medidas disciplinarias, que pueden incluir desde advertencias hasta la terminación del contrato, dependiendo de la gravedad del incumplimiento.

Política de Gestión de Acceso con Permisos Documentales

1. **Propósito**

2. Establecer directrices para controlar el acceso a la documentación de los proyectos, garantizando que solo el personal autorizado pueda acceder a información crítica como planes, cronogramas y actas de reuniones, protegiendo la confidencialidad, integridad y disponibilidad de los datos.

3. **Alcance**

Esta política aplica a todos los empleados, contratistas y terceros que requieran acceso a documentos relacionados con proyectos en las plataformas de gestión documental aprobadas por la organización.

4. **Directrices de la Política**

- **Control de Acceso Basado en Roles (RBAC):**
  - El acceso a los documentos del proyecto se asignará con base en las responsabilidades del usuario.
  - Cada usuario solo tendrá acceso a los documentos necesarios para cumplir con sus funciones.
- **Plataforma de Gestión Documental:**
  - Se utilizará un sistema de gestión documental seguro como Google Drive, SharePoint o un sistema similar que permita:
    - Control granular de permisos (lectura, edición, descarga, eliminación).
    - Registro de actividad para monitorear accesos y modificaciones.
- **Revisión Periódica de Permisos:**
  - Los permisos de acceso serán revisados trimestralmente o cuando ocurran cambios en los roles del personal.
  - Los accesos de usuarios que ya no forman parte del proyecto serán revocados de inmediato.
- **Acceso Temporal:**
  - Cualquier acceso temporal deberá ser aprobado por el gerente del proyecto y tendrá una fecha límite especificada.

4. **Implementación y Supervisión**

- **Solicitud de Acceso:**
  - El personal que necesite acceso a la documentación del proyecto deberá enviar una solicitud al administrador de la plataforma indicando el motivo y el nivel de acceso requerido.
- **Monitoreo de Actividades:**
  - El administrador de la plataforma revisará los registros de actividad para identificar accesos sospechosos o no autorizados.
  - Las actividades inusuales serán reportadas al gerente del proyecto y al equipo de seguridad.

5. **Auditoría y Revisión**

- Se realizarán auditorías trimestrales para:
  - Verificar la validez de los accesos existentes.
  - Identificar y corregir posibles irregularidades.

- Los resultados de las auditorías serán documentados y compartidos con el equipo de seguridad y gerencia.

6. **Sanciones por Incumplimiento**
   El acceso no autorizado, la divulgación indebida de documentos o el incumplimiento de esta política resultarán en medidas disciplinarias, que pueden incluir:

- Suspensión temporal del acceso al sistema.
- Sanciones administrativas o legales en casos graves.

7. **Excepciones**
   Cualquier excepción a esta política deberá ser aprobada por el gerente del proyecto y registrada formalmente, indicando las razones y las medidas alternativas para mitigar riesgos.

8. **Evidencias**

- Registro de accesos configurados en el sistema de gestión documental, detallando el nivel de permisos asignados a cada usuario.
- Informes de auditorías periódicas sobre la gestión de accesos.
- Registros de actividad que demuestren la implementación del monitoreo continuo.

Política de Gestión para Auditoria en Documentos Administrativos

1. **Propósito**

2. El propósito de esta política es garantizar la confidencialidad, integridad y disponibilidad de los documentos administrativos críticos, como presupuestos, contratos, informes financieros y actas de reuniones, mediante la implementación de controles adecuados de acceso, protección y respaldo.

3. **Alcance**

Esta política aplica a todos los empleados, contratistas y terceros con acceso a documentos administrativos, tanto en formato físico como digital, almacenados en sistemas de gestión documental, servidores locales o servicios en la nube utilizados por la empresa.

4. **Requisitos de Gestión de Documentos**

- **Auditoria de Documentos:**
  - Los documentos deben estar administrados en la carpeta raíz para usar la configuración de Quest y tener un manejo más sencillo
- **Auditorías de Acceso:**

- Implementar un registro automático de accesos, modificaciones y eliminaciones de documentos.
- Revisar los registros al menos una vez al mes para identificar actividades sospechosas.

4. **Revisión y Auditoría**

- **Auditorías Periódicas:**
  - Se realizarán auditorías semestrales para verificar el cumplimiento de esta política.
  - Cualquier incumplimiento será reportado al Comité de Seguridad de la Información para su resolución.
- **Evaluación estado del documento:**
  - Los permisos de acceso, modificaciones y eliminaciones del documento.

5. **Responsabilidades**

- **Responsabilidad de los Usuarios:**
  - Reportar cualquier incidente de seguridad relacionado con los documentos a la Dirección de TI.
- **Responsabilidad de la Dirección de TI:**
  - Configurar y mantener los sistemas de gestión documental según las mejores prácticas de seguridad.
  - Implementar y supervisar los registros de acceso y las auditorías periódicas.

6. **Excepciones**
   Cualquier excepción a esta política debe ser aprobada por el Comité de Seguridad de la Información tras una evaluación de riesgos.
7. **Sanciones**
   El incumplimiento de esta política puede dar lugar a medidas disciplinarias, que van desde advertencias hasta la terminación del contrato, dependiendo de la gravedad de la infracción.

Política de Protección de Datos Sensibles

1. **Propósito**

2. El propósito de esta política es garantizar la protección de los datos sensibles de la empresa, como presupuestos, información personal de clientes, proveedores y empleados, y otros documentos confidenciales, mediante el uso de cifrado. De esta forma, se asegura que solo las personas autorizadas puedan acceder y leer dicha información, incluso si los datos son interceptados o accedidos sin autorización.

3. **Alcance**

Esta política aplica a todos los empleados, contratistas y terceros que gestionan o tienen acceso a datos sensibles de la empresa. Cubre tanto los datos almacenados en dispositivos locales (computadoras, servidores) como en servicios en la nube.

4. **Requisitos de Cifrado**

- **Uso Obligatorio de VeraCrypt:**
    - Todos los documentos sensibles deberán ser cifrados utilizando VeraCrypt, una herramienta de cifrado de disco de código abierto.
    - Los documentos críticos como presupuestos, contratos, datos personales y financieros deberán ser almacenados en volúmenes cifrados en VeraCrypt.
- **Tipos de Documentos Sensibles a Cifrar:**
    - Presupuestos de proyectos y contratos con proveedores o clientes.
    - Datos personales de clientes, proveedores y empleados (nombres completos, direcciones, números de contacto, etc.).
    - Informes financieros confidenciales y cualquier otro documento que contenga información sensible.
- **Gestión de Contraseñas:**
    - Las contraseñas de los volúmenes cifrados deben ser gestionadas de manera segura y solo deben ser conocidas por personas autorizadas.
    - El uso de contraseñas fuertes y únicas es obligatorio. Las contraseñas no deben ser compartidas de manera insegura (como en notas físicas o mensajes de texto).
- **Acceso Restringido:**
    - El acceso a los documentos cifrados debe limitarse solo a las personas que necesiten acceder a ellos según su rol o función.
    - El acceso debe ser revocado inmediatamente cuando ya no sea necesario, como en el caso de cambios de rol o salida de personal.

4. **Revisión y Auditoría**

- **Monitoreo de Accesos a Documentos Cifrados:**
    - Se debe llevar un registro de los accesos a los volúmenes cifrados para garantizar que solo personas autorizadas estén accediendo a la información.
    - Las auditorías de acceso a documentos cifrados se realizarán periódicamente para detectar posibles violaciones o accesos no autorizados.

5. **Responsabilidades**

- **Responsabilidad de los Usuarios:**
    - Los usuarios son responsables de cifrar los documentos sensibles utilizando VeraCrypt antes de almacenarlos en cualquier dispositivo.
    - Los usuarios deben garantizar que las contraseñas utilizadas para los volúmenes cifrados sean seguras y estén protegidas.
- **Responsabilidad de los Administradores de TI:**
    - Los administradores de TI deben asegurarse de que la herramienta VeraCrypt esté instalada y actualizada en todos los sistemas pertinentes.
    - Los administradores deben gestionar el acceso a los volúmenes cifrados y garantizar que solo personas autorizadas puedan acceder a los documentos sensibles.

6. **Excepciones**
   Cualquier excepción a esta política debe ser solicitada por escrito a la Dirección de TI, quien evaluará la solicitud según el nivel de riesgo y las necesidades de seguridad de la empresa.
7. **Sanciones**
   El incumplimiento de esta política puede resultar en medidas disciplinarias, que pueden incluir advertencias, sanciones o la terminación del contrato, dependiendo de la gravedad de la infracción.

Política de Control de Acceso al Área de Materiales

1. **Propósito**

2. El propósito de esta política es establecer un control estricto sobre el acceso y retiro de materiales del área de almacenamiento, con el fin de garantizar que solo las personas autorizadas puedan retirar materiales, y que dichos retiros estén debidamente justificados. Esto permitirá una correcta gestión del inventario y garantizará la integridad del stock.

3. **Alcance**

Esta política se aplica a todos los empleados, contratistas y terceros que accedan al área de materiales de la empresa. También cubre el uso del sistema de registro de accesos para controlar y justificar el retiro de materiales de la empresa.

4. **Requisitos del Control de Acceso**

- **Registro Obligatorio de Accesos:**

- Toda persona que desee acceder al área de materiales deberá registrar la siguiente información en un sistema de control de acceso (digital o físico):
    - **Nombre del responsable:** El nombre de la persona que retira los materiales.
    - **Área o departamento:** El departamento al que pertenece el solicitante, para justificar el uso de los materiales.
    - **Materiales a retirar:** Descripción detallada de los materiales, cantidad y, si es posible, códigos o identificadores de los mismos.
    - **Razón o justificación del retiro:** Se debe especificar el motivo por el cual se retiran los materiales (por ejemplo, mantenimiento, instalación en proyecto, reposición de stock).

- **Acceso Exclusivo a Personal Autorizado:**
    - Solo el personal autorizado podrá realizar el retiro de materiales. El acceso a áreas de materiales debe ser restringido a aquellos que cuenten con la debida autorización según su rol y función.
- **Control de Movimientos de Inventario:**
    - Cada retiro de materiales debe estar debidamente registrado y debe ser validado contra los registros de inventario. Se deben registrar también las devoluciones de materiales al área de almacenamiento, si aplicable.

4. Revisión y Auditoría

- **Revisión Periódica de Registros de Acceso:**
    - Se llevará a cabo una revisión periódica de los registros de accesos a materiales, comparándolos con los inventarios para asegurar que no haya discrepancias.
    - Esta revisión será realizada al menos una vez al mes por el responsable del área de inventarios o un auditor externo designado.
- **Auditoría de Materiales Retirados:**
    - Las auditorías de inventario se realizarán al menos dos veces al año para verificar la coherencia entre los materiales registrados y los realmente disponibles en el inventario físico.

5. Responsabilidades

- **Responsabilidad del Personal Autorizado:**
    - Cada persona autorizada para retirar materiales es responsable de registrar correctamente los datos de acceso al área de materiales y justificar de manera adecuada el motivo de retiro.

    - El personal debe seguir rigurosamente las directrices de esta política y garantizar que los materiales retirados sean utilizados exclusivamente para los fines autorizados.
- **Responsabilidad del Departamento de Inventarios:**
    - El departamento encargado de los inventarios es responsable de mantener el sistema de registro actualizado, auditar los accesos y revisar periódicamente los registros para garantizar la correcta gestión de los materiales.
    - Además, debe realizar auditorías periódicas y gestionar las excepciones o discrepancias que se detecten en los registros.

6. **Excepciones**
   Cualquier solicitud de excepción a esta política debe ser solicitada por escrito y debe ser aprobada por el jefe del departamento de inventarios. Las excepciones se evaluarán según la naturaleza del caso y los riesgos asociados.
7. **Sanciones**
   El incumplimiento de esta política puede resultar en sanciones, que pueden incluir desde advertencias hasta la suspensión de acceso al área de materiales, dependiendo de la gravedad del incumplimiento. En casos de mal manejo de inventarios o fraudes, pueden aplicarse medidas disciplinarias más severas, incluyendo la terminación del contrato.

Política de Limpieza de Escritorio

1. **Propósito**

2. El propósito de esta política es garantizar la seguridad de la información sensible y confidencial al implementar prácticas que minimicen el riesgo de exposición no autorizada. Esto incluye documentos físicos, dispositivos electrónicos y cualquier otro medio que contenga información crítica.

3. **Alcance**

Esta política aplica a todos los empleados, contratistas y terceros que utilicen espacios de trabajo dentro de las instalaciones de la empresa. Es obligatoria para oficinas, áreas comunes, salas de reuniones y cualquier espacio donde se maneje información sensible.

4. **Directrices de la Política de Limpieza de Escritorio**

- **Documentos Físicos:**

    - Al final del día, todo documento con información sensible o confidencial debe ser guardado en un lugar seguro, como gabinetes cerrados o archivadores con llave.
    - Los documentos que ya no sean necesarios deben ser destruidos mediante un método seguro, como trituradores de papel.
- **Equipos Electrónicos:**
    - Los dispositivos como laptops, tablets y teléfonos móviles deben estar bloqueados con contraseñas seguras y guardados en un lugar seguro cuando no estén en uso.
    - Las pantallas de las computadoras deben estar apagadas o bloqueadas si el usuario se ausenta del escritorio por más de 5 minutos.
- **Objetos Personales:**
    - Los empleados deben evitar dejar objetos personales no necesarios en sus escritorios que puedan ser fuente de distracción o facilitar accesos no autorizados.
- **Material de Oficina:**
    - Cualquier material de oficina que contenga información de clientes, contratos o datos sensibles debe estar debidamente asegurado.

4. Implementación y Supervisión

- **Responsabilidad del Personal:**
    - Cada empleado es responsable de mantener limpio y seguro su espacio de trabajo al final de cada jornada laboral.
    - Deben reportar cualquier pérdida o exposición de información a su supervisor inmediato.
- **Responsabilidad del Departamento de Seguridad:**
    - Realizar inspecciones regulares para verificar el cumplimiento de esta política.
    - Proveer gabinetes, cerraduras y otros recursos necesarios para que los empleados aseguren sus materiales.

5. Auditoría y Revisión

- Se realizarán auditorías mensuales para evaluar el cumplimiento de la política y detectar posibles puntos de mejora.
- En caso de detectar incumplimientos, se notificará al empleado responsable y se implementarán medidas correctivas.

6. **Sanciones por Incumplimiento**

El incumplimiento de esta política puede resultar en:

- Una advertencia verbal o escrita en caso de primera infracción.
- Medidas disciplinarias más severas para incumplimientos repetidos o que comprometan información crítica.

7. **Excepciones**
   Cualquier excepción a esta política debe ser solicitada al área de Recursos Humanos o al Departamento de TI y aprobada por escrito, especificando las razones y los controles alternativos a implementarse.