

**Manual de Procedimientos de Seguridad de la Información**

**Índice**

1. **Introducción**
	* Propósito y alcance
	* Definiciones clave
	* Revisión y actualización periódica
2. **Gobernanza de la Seguridad de la Información**
	* Estructura organizativa
	* Roles y responsabilidades
	* Comité de Seguridad de la Información
3. **Gestión de Activos**
	* Clasificación de la información
	* Manejo de medios
	* Control de inventario
4. **Control de Acceso**
	* Política de control de acceso
	* Gestión de identidades y credenciales
	* Control de acceso físico y lógico
5. **Gestión de la Operatividad**
	* Procedimientos y responsabilidades operativas
	* Gestión de cambios y configuraciones
	* Respaldo y recuperación de datos
6. **Seguridad en Recursos Humanos**
	* Durante la contratación
	* Durante el empleo
	* Terminación o cambio de empleo
7. **Seguridad Física y del Entorno**
	* Seguridad perimetral
	* Protección contra amenazas externas e internas
	* Seguridad ambiental
8. **Gestión de Comunicaciones y Operaciones**
	* Procedimientos de gestión de redes
	* Transferencia de información
	* Mensajería electrónica y almacenamiento en la nube
9. **Adquisición, Desarrollo y Mantenimiento de Sistemas**
	* Requisitos de seguridad en sistemas de información
	* Seguridad en el desarrollo y soporte de aplicaciones
	* Vulnerabilidades técnicas
10. **Gestión de Incidentes de Seguridad de la Información**
	* Reporte de eventos y debilidades
	* Respuesta a incidentes de seguridad de la información
	* Aprendizaje y mejora continua
11. **Gestión de la Continuidad del Negocio**
	* Aspectos de la seguridad de la información en la gestión de la continuidad
	* Planes de continuidad y recuperación
12. **Cumplimiento**
	* Cumplimiento con políticas y normativas
	* Revisión de la seguridad de la información
	* Auditorías de seguridad de la información

**Introducción**

**Propósito y Alcance**

**Propósito**

En [**Nombre de la Empresa**], reconocemos la importancia crítica de proteger nuestra información y la de nuestros clientes. Por ello, hemos desarrollado este Manual de Procedimientos de Seguridad de la Información. Nuestro objetivo es garantizar la confidencialidad, integridad y disponibilidad de todos los datos e información que manejamos, minimizando así los riesgos de seguridad y asegurando la continuidad de nuestras operaciones.

Este manual es un componente esencial de nuestra estrategia de seguridad y sirve como guía para todos los empleados y colaboradores. A través de él, establecemos las prácticas estándar que deben seguirse para proteger nuestra información y sistemas de cualquier amenaza o vulnerabilidad.

**Alcance**

El alcance de este manual abarca todos los aspectos relacionados con la seguridad de la información en [**Nombre de la Empresa**]. Esto incluye, pero no se limita a:

* **Datos Corporativos:** Toda la información generada, procesada, almacenada o transmitida por [**Nombre de la Empresa**], incluyendo datos financieros, de clientes, de empleados y propiedad intelectual.
* **Sistemas y Redes:** Todos los sistemas informáticos, redes, dispositivos móviles y cualquier otro medio tecnológico utilizado para el procesamiento y almacenamiento de datos.
* **Empleados y Colaboradores:** Todas las personas que tienen acceso a nuestros sistemas y datos, incluyendo empleados, contratistas, socios comerciales y otros terceros.
* **Instalaciones Físicas:** Todas las ubicaciones y entornos físicos desde donde se accede a la información de la empresa, incluyendo oficinas centrales, sucursales, centros de datos y espacios de trabajo remotos.

Este manual se aplica a todas las operaciones de [**Nombre de la Empresa**] y es de obligado cumplimiento para todos los empleados y colaboradores. Además, es responsabilidad de cada miembro del equipo familiarizarse con estas políticas y procedimientos, y adherirse a ellos en su actividad diaria.

En [**Nombre de la Empresa**], estamos comprometidos con la mejora continua de nuestras prácticas de seguridad de la información. Por lo tanto, este manual está sujeto a revisiones y actualizaciones periódicas para reflejar los cambios en la tecnología, las amenazas emergentes, las nuevas regulaciones y las mejores prácticas de la industria.

**Definiciones Clave**

En [**Nombre de la Empresa**], utilizamos terminología específica en relación con la seguridad de la información. A continuación, se presentan definiciones clave para garantizar una comprensión uniforme y clara de estos términos en todo nuestro manual y prácticas:

1. **Confidencialidad:** Se refiere a la protección de la información para evitar su divulgación no autorizada. Nos aseguramos de que solo las personas autorizadas tengan acceso a la información confidencial.
2. **Integridad:** La exactitud y completitud de la información y los métodos de procesamiento. En [**Nombre de la Empresa**], garantizamos que nuestra información no sea alterada o corrompida de manera no autorizada.
3. **Disponibilidad:** Asegurar que la información y los recursos asociados estén accesibles para los usuarios autorizados cuando lo necesiten. Nos esforzamos por mantener nuestros sistemas operativos y disponibles en todo momento.
4. **Amenaza:** Cualquier circunstancia o evento con el potencial de causar daño a nuestros sistemas de información o a la información misma. Las amenazas pueden ser internas o externas, intencionadas o accidentales.
5. **Vulnerabilidad:** Una debilidad en nuestros sistemas o procesos que podría ser explotada por una amenaza. Identificar y mitigar vulnerabilidades es clave para fortalecer nuestra seguridad.
6. **Riesgo:** La posibilidad de que una amenaza explote una vulnerabilidad, causando un impacto negativo en la organización. La gestión de riesgos implica identificar, evaluar y mitigar riesgos para reducirlos a un nivel aceptable.
7. **Control de Seguridad:** Medidas adoptadas para proteger la información y los sistemas de información. Estos controles pueden ser técnicos, como el cifrado, o administrativos, como las políticas y procedimientos.
8. **Gestión de Incidentes:** El proceso de identificar, gestionar, registrar y analizar los incidentes de seguridad en [**Nombre de la Empresa**] para prevenir futuras ocurrencias.
9. **Cumplimiento:** Asegurar que [**Nombre de la Empresa**] cumpla con todas las leyes, regulaciones, políticas y estándares aplicables a la seguridad de la información.
10. **Evaluación de Riesgos:** El proceso de identificar y evaluar los riesgos para la seguridad de la información, considerando la probabilidad y el impacto de un evento de seguridad.
11. **Cifrado:** La técnica de convertir información o datos en un código para prevenir accesos no autorizados o lecturas.
12. **Autenticación y Autorización:** Procesos para verificar la identidad de un usuario (autenticación) y determinar su acceso a recursos específicos (autorización).

Estas definiciones son fundamentales para entender y aplicar correctamente las políticas y procedimientos descritos en este manual. En [**Nombre de la Empresa**], nos comprometemos a mantener un lenguaje claro y consistente para asegurar que todos los miembros del equipo comprendan y apliquen efectivamente nuestras prácticas de seguridad de la información.

**Revisión y Actualización Periódica**

**Proceso de Revisión**

En [**Nombre de la Empresa**], entendemos que el entorno de seguridad de la información es dinámico y en constante evolución. Por ello, es esencial mantener nuestro Manual de Procedimientos de Seguridad de la Información actualizado. Este documento no es estático; es un recurso en constante evolución que refleja los cambios en las amenazas de seguridad, la tecnología, las regulaciones y las mejores prácticas de la industria.

El proceso de revisión se lleva a cabo de la siguiente manera:

1. **Revisión Regular:** El manual se revisa de manera integral al menos una vez al año. Sin embargo, componentes específicos pueden ser revisados con mayor frecuencia, según sea necesario.
2. **Evaluación de Cambios en el Entorno:** Monitoreamos continuamente el entorno de seguridad de la información para identificar cualquier cambio que pueda afectar nuestras políticas y procedimientos, incluyendo nuevas amenazas, vulnerabilidades emergentes, avances tecnológicos y cambios en la legislación.
3. **Contribuciones de los Empleados:** Fomentamos una cultura de seguridad donde todos los empleados están invitados a proporcionar retroalimentación y sugerencias sobre las prácticas de seguridad. Esta retroalimentación se considera cuidadosamente durante las revisiones del manual.
4. **Revisión por Expertos:** Las revisiones son realizadas por un equipo de expertos en seguridad de la información, incluyendo a miembros del departamento de TI, seguridad, legal y recursos humanos, para garantizar una perspectiva integral.
5. **Aprobación y Comunicación:** Una vez revisado, el manual es aprobado por la alta dirección. Las actualizaciones son comunicadas a todos los empleados y partes interesadas relevantes a través de los canales apropiados, como reuniones, correos electrónicos internos o plataformas de comunicación de la empresa.

**Actualizaciones Continuas**

Además de las revisiones periódicas, el manual puede ser actualizado en respuesta a eventos específicos, como:

* Incidentes de seguridad significativos.
* Cambios importantes en la infraestructura o prácticas de TI de la empresa.
* Nuevas leyes o regulaciones que afecten la seguridad de la información.

**Capacitación y Concienciación**

Tras cada actualización, organizamos sesiones de capacitación y concienciación para asegurarnos de que todos los empleados comprendan las nuevas políticas y procedimientos. Estas sesiones son cruciales para mantener una cultura de seguridad robusta en [**Nombre de la Empresa**].

**Registro de Cambios**

Mantenemos un registro detallado de todas las revisiones y actualizaciones para proporcionar un historial claro de los cambios y asegurar la transparencia en nuestro enfoque de la seguridad de la información.

En [**Nombre de la Empresa**], el compromiso con la seguridad de la información es una responsabilidad compartida, y la revisión y actualización periódica de nuestro Manual de Procedimientos de Seguridad de la Información es fundamental para proteger nuestros activos digitales y la confianza de nuestros clientes y socios.

**Gobernanza de la Seguridad de la Información**

**Estructura Organizativa**

En [**Nombre de la Empresa**], la estructura organizativa para la gobernanza de la seguridad de la información está diseñada para garantizar una gestión eficaz y eficiente de los riesgos relacionados con la información y para promover una cultura de seguridad en toda la organización. Nuestra estructura se caracteriza por los siguientes elementos:

1. **Alta Dirección:** La responsabilidad última de la seguridad de la información recae en la alta dirección, que proporciona la dirección estratégica y los recursos necesarios. La alta dirección está comprometida en establecer y promover la cultura de seguridad dentro de la empresa.
2. **Oficial de Seguridad de la Información (OSI):** Designamos un Oficial de Seguridad de la Información, quien es responsable de supervisar y coordinar todas las actividades relacionadas con la seguridad de la información. El OSI actúa como el punto central para todas las cuestiones de seguridad y trabaja en estrecha colaboración con diferentes departamentos para garantizar la implementación efectiva de las políticas y procedimientos de seguridad.
3. **Equipo de Seguridad de la Información:** Este equipo está compuesto por profesionales especializados en diferentes áreas de la seguridad de la información, como la gestión de riesgos, la seguridad cibernética, el cumplimiento normativo y la respuesta a incidentes. Trabajan bajo la dirección del OSI para implementar estrategias de seguridad, realizar evaluaciones de riesgos y responder a incidentes de seguridad.
4. **Comités de Seguridad de la Información:** Establecemos comités que involucran a representantes de varios departamentos, como TI, recursos humanos, legal y operaciones. Estos comités se reúnen regularmente para discutir y revisar las políticas de seguridad, abordar nuevos desafíos y garantizar que las prácticas de seguridad se alineen con los objetivos empresariales.
5. **Roles y Responsabilidades Definidos:** Cada empleado en [**Nombre de la Empresa**] tiene responsabilidades definidas en relación con la seguridad de la información. Estas responsabilidades están claramente documentadas y comunicadas a través de políticas, procedimientos y programas de capacitación.
6. **Colaboración Interdepartamental:** Fomentamos una colaboración estrecha entre diferentes departamentos para garantizar una comprensión integral de los riesgos de seguridad y para implementar controles efectivos en toda la organización.
7. **Comunicación y Reporte:** Mantenemos canales de comunicación efectivos para reportar y discutir asuntos relacionados con la seguridad de la información. Esto incluye reportes regulares a la alta dirección, así como comunicaciones a todos los niveles de la organización.
8. **Formación y Concienciación:** Implementamos programas continuos de formación y concienciación en seguridad de la información para todos los empleados. Estos programas están diseñados para mantener al personal informado sobre las últimas amenazas, mejores prácticas y responsabilidades individuales.

En [**Nombre de la Empresa**], la estructura organizativa para la gobernanza de la seguridad de la información es un pilar fundamental para proteger nuestros activos de información y para asegurar la confianza de nuestros clientes y socios. Nos comprometemos a mantener una estructura robusta y adaptativa que responda a los cambiantes desafíos de seguridad en el entorno digital actual.

**Roles y Responsabilidades en la Gobernanza de la Seguridad de la Información**

En [**Nombre de la Empresa**], la efectividad de nuestra gobernanza de seguridad de la información depende de la clara definición y asignación de roles y responsabilidades. Estos roles están diseñados para garantizar que todos los aspectos de la seguridad de la información sean gestionados de manera efectiva y coherente en toda la organización.

1. **Alta Dirección:**
	* Establecer la visión y estrategia general de seguridad de la información.
	* Asegurar la asignación de recursos adecuados para la seguridad de la información.
	* Promover una cultura de seguridad en toda la organización.
	* Tomar decisiones clave en relación con la gestión de riesgos y la respuesta a incidentes.
2. **Oficial de Seguridad de la Información (OSI):**
	* Desarrollar y mantener el marco de políticas de seguridad de la información.
	* Coordinar la implementación de las prácticas de seguridad en toda la empresa.
	* Supervisar la evaluación de riesgos y la gestión de incidentes.
	* Informar a la alta dirección sobre el estado de la seguridad de la información.
3. **Equipo de Seguridad de la Información:**
	* Implementar y mantener las medidas de seguridad técnicas.
	* Realizar auditorías y pruebas de seguridad regulares.
	* Gestionar la respuesta a incidentes de seguridad y recuperación.
	* Proporcionar asesoramiento y soporte técnico en cuestiones de seguridad.
4. **Departamento de Tecnologías de la Información (TI):**
	* Asegurar la seguridad de la infraestructura y los sistemas de TI.
	* Implementar controles de acceso y medidas de protección de datos.
	* Mantener sistemas actualizados y parcheados contra vulnerabilidades.
	* Colaborar en la respuesta a incidentes y en la recuperación de sistemas.
5. **Departamento de Recursos Humanos:**
	* Gestionar la seguridad de la información en relación con los empleados.
	* Asegurar que las políticas de seguridad sean parte de los contratos y acuerdos laborales.
	* Coordinar la formación y concienciación en seguridad de la información.
	* Gestionar el proceso de salida de empleados para asegurar la protección de la información.
6. **Departamento Legal y de Cumplimiento:**
	* Asegurar el cumplimiento de las leyes y regulaciones relacionadas con la seguridad de la información.
	* Gestionar los aspectos legales de los contratos y acuerdos que implican seguridad de la información.
	* Asesorar sobre las implicaciones legales de incidentes de seguridad.
7. **Todos los Empleados:**
	* Cumplir con las políticas y procedimientos de seguridad de la información.
	* Reportar cualquier actividad sospechosa o incidentes de seguridad.
	* Participar en formaciones y estar al tanto de las mejores prácticas de seguridad.
8. **Socios y Proveedores:**
	* Asegurar que cumplan con nuestras políticas de seguridad de la información.
	* Reportar cualquier incidente de seguridad que afecte a [**Nombre de la Empresa**].
	* Mantener una comunicación abierta sobre riesgos y medidas de seguridad.

En [**Nombre de la Empresa**], entendemos que la seguridad de la información es una responsabilidad compartida. Cada miembro de nuestro equipo, desde la alta dirección hasta el personal de nivel de entrada, juega un papel vital en la protección de nuestros activos de información. La colaboración y el compromiso continuo con estas responsabilidades son fundamentales para mantener la integridad, confidencialidad y disponibilidad de nuestra información.

**Comité de Seguridad de la Información**

En [**Nombre de la Empresa**], el Comité de Seguridad de la Información desempeña un papel crucial en la gobernanza de la seguridad de nuestra información. Este comité es un grupo multidisciplinario que reúne a líderes y expertos de diferentes áreas de la empresa para asegurar un enfoque integral y coherente en la gestión de la seguridad de la información.

**Funciones y Responsabilidades del Comité:**

1. **Desarrollo de Estrategias y Políticas:**
	* El comité es responsable de desarrollar la estrategia general de seguridad de la información de la empresa.
	* Revisa y aprueba políticas y procedimientos de seguridad, asegurándose de que estén alineados con los objetivos empresariales y las regulaciones vigentes.
2. **Evaluación y Gestión de Riesgos:**
	* Realiza evaluaciones regulares de riesgos de seguridad de la información para identificar y priorizar riesgos potenciales.
	* Recomienda medidas para mitigar los riesgos identificados y supervisa la implementación de estas medidas.
3. **Supervisión y Revisión de Controles:**
	* Supervisa la implementación y eficacia de los controles de seguridad en toda la organización.
	* Revisa periódicamente los controles existentes para asegurar que sigan siendo relevantes y efectivos frente a las amenazas cambiantes.
4. **Coordinación entre Departamentos:**
	* Facilita la coordinación y comunicación entre diferentes departamentos, asegurando que todos los aspectos de la seguridad de la información sean considerados y gestionados de manera efectiva.
	* Promueve una cultura de seguridad en toda la organización, asegurando que la seguridad de la información sea una responsabilidad compartida.
5. **Formación y Concienciación:**
	* Asegura que se implementen programas de formación y concienciación en seguridad de la información para todos los empleados.
	* Promueve la educación continua y la sensibilización sobre las mejores prácticas de seguridad y las amenazas emergentes.
6. **Respuesta a Incidentes:**
	* Desarrolla y mantiene un plan de respuesta a incidentes de seguridad de la información.
	* Coordina la respuesta a incidentes de seguridad y supervisa la investigación y resolución de estos.
7. **Reporte y Comunicación:**
	* Reporta regularmente a la alta dirección sobre el estado de la seguridad de la información en la empresa.
	* Comunica las actualizaciones importantes y los cambios en las políticas de seguridad a todos los empleados y partes interesadas.

**Composición del Comité:**

El Comité de Seguridad de la Información está compuesto por miembros de alto nivel de varios departamentos, incluyendo, pero no limitándose a, TI, Recursos Humanos, Legal, Cumplimiento, y Operaciones. El Oficial de Seguridad de la Información (OSI) generalmente preside el comité.

En [**Nombre de la Empresa**], el Comité de Seguridad de la Información es fundamental para garantizar que nuestra estrategia y prácticas de seguridad de la información sean robustas, coherentes y efectivas. A través de su liderazgo y orientación, nos esforzamos por proteger nuestros activos de información y mantener la confianza de nuestros clientes y socios.

**Gestión de Activos**

**Clasificación de la Información**

En [**Nombre de la Empresa**], la clasificación de la información es un proceso esencial para garantizar que nuestros datos se manejen y protejan adecuadamente. La clasificación proporciona una base para aplicar los controles de seguridad apropiados y garantizar que la información crítica para la empresa reciba el nivel más alto de protección.

**Proceso de Clasificación de la Información:**

1. **Identificación de la Información:**
	* Realizamos un inventario completo de todos los tipos de información que manejamos, incluyendo datos digitales y físicos.
	* Identificamos la fuente, el uso y la importancia de cada tipo de información para las operaciones de la empresa.
2. **Criterios de Clasificación:**
	* Establecemos criterios claros para la clasificación basados en la sensibilidad y el valor de la información.
	* Los criterios comunes incluyen la confidencialidad, la integridad y la disponibilidad de la información.
3. **Niveles de Clasificación:**
	* Definimos varios niveles de clasificación, como 'Público', 'Interno', 'Confidencial' y 'Altamente Confidencial'.
	* Cada nivel tiene asociado un conjunto de controles de seguridad y procedimientos de manejo.
4. **Asignación de Clasificación:**
	* Asignamos un nivel de clasificación a cada tipo de información basándonos en los criterios establecidos.
	* La clasificación es realizada por personal capacitado que comprende el valor y la sensibilidad de la información.
5. **Etiquetado y Manejo:**
	* Etiquetamos claramente la información con su nivel de clasificación correspondiente.
	* Proporcionamos directrices sobre cómo manejar, almacenar y compartir cada nivel de información clasificada.
6. **Revisión y Actualización:**
	* Revisamos periódicamente la clasificación de la información para asegurar que sigue siendo relevante y precisa.
	* Actualizamos la clasificación en respuesta a cambios en el entorno de negocio o en las regulaciones.

**Responsabilidades de los Empleados:**

* Todos los empleados son responsables de clasificar correctamente la información que crean o manejan.
* Se espera que los empleados sigan las políticas y procedimientos establecidos para el manejo de información clasificada.
* Los empleados deben recibir formación regular sobre la importancia de la clasificación de la información y cómo aplicarla en su trabajo diario.

**Auditorías y Cumplimiento:**

* Realizamos auditorías regulares para asegurar que la clasificación de la información se esté llevando a cabo correctamente y que se estén siguiendo los procedimientos de manejo.
* Las violaciones de las políticas de clasificación de la información son tratadas seriamente y pueden resultar en acciones disciplinarias.

En [**Nombre de la Empresa**], la clasificación efectiva de la información es fundamental para proteger nuestros activos de información y para garantizar que se manejen de manera segura y eficiente. Este proceso nos ayuda a identificar qué información requiere mayor protección y a asignar recursos de seguridad de manera adecuada.

**Gestión de Activos**

**Manejo de Medios**

En [**Nombre de la Empresa**], el manejo adecuado de los medios es una parte integral de nuestra estrategia de seguridad de la información. Los medios, que incluyen dispositivos de almacenamiento físico y digital, así como documentos impresos, contienen información valiosa y a menudo sensible. Por lo tanto, es crucial gestionarlos de manera segura para proteger la información que contienen.

**Procedimientos para el Manejo de Medios:**

1. **Uso y Manejo Adecuado:**
	* Establecemos directrices claras sobre el uso adecuado de los medios de almacenamiento, como discos duros, unidades USB, CD/DVD, y dispositivos móviles.
	* Los empleados reciben formación sobre cómo manejar estos medios de forma segura, incluyendo el almacenamiento y la transferencia de datos.
2. **Etiquetado y Registro:**
	* Todos los medios se etiquetan claramente con su nivel de clasificación de información.
	* Mantenemos un registro de todos los medios utilizados, incluyendo su ubicación y la persona responsable de ellos.
3. **Almacenamiento Seguro:**
	* Los medios que contienen información confidencial o sensible se almacenan en áreas seguras con acceso restringido.
	* Implementamos controles físicos y electrónicos para proteger estos medios de accesos no autorizados o daños.
4. **Transferencia de Medios:**
	* La transferencia de medios dentro y fuera de la empresa se realiza bajo estrictas políticas de seguridad.
	* Utilizamos métodos seguros de transferencia y aseguramos que solo el personal autorizado pueda transportar medios sensibles.
5. **Eliminación y Destrucción:**
	* Cuando los medios ya no son necesarios, se eliminan o destruyen de manera segura y conforme a las políticas de la empresa.
	* Para medios digitales, utilizamos métodos de borrado que garantizan que los datos no puedan ser recuperados. Para documentos impresos y medios físicos, empleamos métodos de destrucción como trituradoras o incineración.
6. **Respuesta a Incidentes:**
	* En caso de pérdida o robo de medios, tenemos procedimientos establecidos para responder rápidamente y mitigar cualquier posible fuga de información.
	* Estos incidentes se registran y analizan para mejorar nuestras prácticas de seguridad.
7. **Auditorías y Revisiones:**
	* Realizamos auditorías periódicas para asegurar que los procedimientos de manejo de medios se sigan correctamente.
	* Las revisiones nos ayudan a identificar y corregir cualquier debilidad en nuestras prácticas de manejo de medios.

**Concienciación y Capacitación del Personal:**

* La formación y concienciación continua del personal son esenciales para garantizar que todos los empleados comprendan la importancia del manejo seguro de los medios.
* Proporcionamos capacitaciones regulares sobre las mejores prácticas y los riesgos asociados con el manejo inadecuado de los medios.

En [**Nombre de la Empresa**], reconocemos que el manejo seguro de los medios es fundamental para proteger nuestra información y prevenir fugas de datos. Nos comprometemos a implementar y mantener prácticas sólidas de manejo de medios para garantizar la seguridad y la integridad de nuestra información.

**Gestión de Activos**

**Control de Inventario**

En [**Nombre de la Empresa**], el control efectivo de inventario es un aspecto crucial de la gestión de activos y la seguridad de la información. Mantener un registro preciso y actualizado de todos los activos de información y los dispositivos asociados nos permite protegerlos de manera efectiva y garantizar su uso adecuado.

**Procedimientos para el Control de Inventario:**

1. **Registro de Activos:**
	* Todos los activos de información, incluyendo hardware, software y medios de almacenamiento, se registran en una base de datos centralizada de inventario.
	* Cada activo se etiqueta con un identificador único y se registra con detalles como su descripción, ubicación, propietario asignado y estado.
2. **Actualizaciones Regulares:**
	* El inventario se actualiza regularmente para reflejar nuevas adquisiciones, cambios o disposiciones de activos.
	* Las actualizaciones también incluyen cambios en la ubicación o en la asignación de responsabilidades de los activos.
3. **Revisión y Auditoría:**
	* Realizamos revisiones periódicas del inventario para asegurar su precisión y completitud.
	* Las auditorías internas o externas ayudan a verificar la exactitud del registro de inventario y a identificar discrepancias.
4. **Control de Acceso:**
	* Restringimos el acceso a la base de datos de inventario a personal autorizado para mantener la integridad de los datos.
	* Implementamos controles de seguridad para proteger la base de datos contra accesos no autorizados o modificaciones.
5. **Gestión del Ciclo de Vida:**
	* Supervisamos el ciclo de vida completo de cada activo, desde su adquisición hasta su disposición.
	* Esto incluye la gestión de licencias de software, mantenimiento de hardware y renovación o eliminación segura de activos.
6. **Responsabilidad del Personal:**
	* Los empleados son responsables de los activos asignados a ellos y deben adherirse a las políticas de uso y seguridad.
	* Se espera que reporten cualquier incidente o cambio relacionado con los activos bajo su responsabilidad.
7. **Disposición Segura:**
	* Cuando un activo ya no es necesario o ha llegado al final de su vida útil, se dispone de él de manera segura.
	* Esto incluye la eliminación de toda la información almacenada y la destrucción física si es necesario, especialmente para medios de almacenamiento.

**Capacitación y Concienciación:**

* Proporcionamos formación regular a los empleados sobre la importancia del control de inventario y su papel en la seguridad de la información.
* Aseguramos que todos los empleados entiendan las políticas y procedimientos relacionados con el manejo y la responsabilidad de los activos de la empresa.

En [**Nombre de la Empresa**], el control de inventario es una parte integral de nuestra estrategia de seguridad de la información. Nos permite no solo proteger nuestros activos físicos y digitales, sino también garantizar que se utilicen y mantengan de manera eficiente y segura. Este enfoque proactivo en la gestión de activos es esencial para mantener la integridad y la seguridad de nuestra información.

**Control de Acceso**

**Política de Control de Acceso**

En [**Nombre de la Empresa**], la política de control de acceso es fundamental para proteger nuestros recursos de información y tecnología. Esta política establece el marco para gestionar cómo los empleados, contratistas y otras partes interesadas acceden a los sistemas y datos de la empresa, asegurando que solo las personas autorizadas tengan acceso a la información relevante y necesaria para sus roles.

**Elementos Clave de la Política de Control de Acceso:**

Principio del formulario