1. OBJETIVO

Garantizar la protección, confidencialidad, integridad y disponibilidad de la información y los datos de la empresa, mediante la implementación de medidas de seguridad adecuadas y el monitoreo constante del sistema. Este procedimiento se aplica a todos los empleados, contratistas y terceros que tengan acceso a la información y datos de la empresa

2. ALCANCE

Este procedimiento se aplica a todos los datos e información relevantes de la empresa, incluyendo información confidencial, financiera y de propiedad intelectual. Además, este procedimiento incluye la implementación y el seguimiento de medidas de seguridad adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la información y los datos. Este procedimiento es aplicable a todos los empleados, contratistas y terceros que tengan acceso a la información y los datos de la empresa, incluyendo los sistemas de información y comunicación, instalaciones y equipos utilizados para el procesamiento y almacenamiento de información y datos de la empresa.

3. RESPONSABILIDAD

- Director de Seguridad de la Información
- Dirección Administrativa

4. TÉRMINOS Y DEFINICIONES

Datos. Hechos sobre los objetos.

Documento. Información y el medio en el que está contenida

Información. Datos que poseen significado

Registro. Documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas. Deben denominarse acorde con la tipología establecida en las Tablas de Retención Documental – TRD, para su conservación

5. POLÍTICAS

De acuerdo con el Manual de Políticas de Seguridad de la Información.

6. DESCRIPCIÓN GENERAL

6.1 Clasificación de la Información

La información se clasifica de acuerdo con los criterios establecidos para la clasificación de activos en el Procedimiento de Identificación de Activos y el Instructivo de Organización de Archivos.

6.2Acceso a la información

6.2.1 Política de control de acceso

La organización establece un control de acceso con base en el resultado y niveles identificados en la Matriz de Riesgos en Seguridad de la Información. La definición de autorización o restricción para uso y consulta de la información, creación o modificación, -incluyendo los sistemas de procesamiento- se hace siguiendo las Políticas de seguridad.
De acuerdo con estas reglas y derechos se tienen dos tipos de restricciones de acceso: físicos y de sistemas de procesamiento.

- **Restricciones de acceso físico**: Restricciones de acceso como puertas, llaves y otros métodos en los puntos de almacenamiento bajo la responsabilidad del dueño de la información (cargos).
- **Restricciones de acceso al sistema de información:** Restricciones a los sistemas de procesamiento administradas por el área de sistemas.

6.2.2 Otorgamiento de acceso a la información

La definición del acceso y distribución de la información es responsabilidad de cada líder de proceso. Los niveles de acceso definidos para los roles y los propietarios de los activos son comunicados al personal.

El control de acceso incluye la identificación de los receptores autorizados o usuarios a quienes se puede entregar la información y la distribución o a quienes se puede enviar la información. Los principios para otorgamiento de acceso a la información son:

- El acceso se determina para los roles no para las personas.
- Los derechos de acceso, distribución y receptores son definidos por cada líder de proceso o director de área.
- El acceso a información secreta debe ser aprobado por la Dirección de la Compañía.
- El número de personas y roles con acceso a información debe mantenerse mínimo acorde con las necesidades de la organización.
- La asignación de derechos de acceso al titular de un cargo solo puede hacerse si cumple con los requisitos del Proceso de Gestión del Talento Humano incluyendo verificación de antecedentes y acuerdo de confidencialidad.
- La asignación de derechos de acceso a contratistas o proveedores se realiza de acuerdo con el Proceso Gestión Administrativa, Contable y Financiera.
- Se da el entrenamiento a empleados y contratistas sobre el manejo de los derechos de acceso y seguridad de la información.
- El propietario de cada activo de información es el responsable primario de mantener la seguridad en casos de necesidad de compartir, distribuir, almacenar y transportar la información
- En caso de necesidad de compartir información no pública con personas internas o externas por fuera de lo establecido, se debe contar con la autorización del líder de proceso, la alta dirección o el director de seguridad de la información.
- El retiro de un empleado o contratista implica también la terminación de los derechos de acceso según, igualmente para cambios en cargo de un empleado.
- El análisis de riesgos, incidentes de seguridad, procesos disciplinarios pueden modificar los derechos de acceso establecidos para la información, cargos y personas con derechos establecidos.
- El acceso remoto a la información o los sistemas de procesamiento debe ser autorizada por el líder de área y cumplir las políticas definidas. El acceso a sitios donde se tiene información o sistema de procesamiento se controla de acuerdo con el Procedimiento de Seguridad Física y del Entorno.

6.2.3 Información disponible al público

La información autorizada para el público es revisada y aprobada por el **Gerente General** y el **Director de Seguridad de Información** según corresponda, con el fin de evaluar:

- Adecuación con los requisitos de la organización y legales (coherente con las políticas de la empresa).
- Confiabilidad de la información suministrada al público (que sea correcta en su contenido).
- Cumplimiento de requisitos de confidencialidad (que información se puede suministrar y a qué público).

La información para el público se suministra por:

- Impresos (volantes, publicaciones, boletines).
- Página www.syscafe.com
- Boletines electrónicos.
- Carteleras.
- Correos electrónicos.

Cuando la información está publicada en la página, el grupo de infraestructura es responsable de la protección para acceso no autorizado o modificación.

6.3 Validación

La validación de la información y datos de entrada, proceso y salida en los sistemas de procesamiento de información se realizan de acuerdo con el proceso pruebas de software, cuando se presentan implementaciones, modificaciones o actualizaciones en los sistemas de procesamiento.

Proceso de pruebas de software

SysCafé como empresa de software dentro de su departamento de desarrollo y proyectos, cuenta con un Analista Tester quien cumple con el seguimiento de los requerimientos desde su puesta en pruebas hasta su culminación exitosa.

El procedimiento consta de revisar los seguimientos en pruebas, revisar los ejecutables y los procesos incorporados en los productos para continuar con el debido testeo.

con el proceso de testeo podemos encontrar dos posibles situaciones:

- **El test o pruebas finaliza con un diagnóstico positivo:** El analista tester realiza todas las pruebas pertinentes aplicando los filtros de testeo funcionales y no funcionales, bajo un mecanismo estandarizado y aprobado por SysCafé, el cual una vez terminado se encuentra que correctamente aplicado, posteriormente se procede con la indicación al funcionario del área correspondiente para su revisión y entrega al usuario final.
- **El test o pruebas finaliza con un diagnóstico negativo:** El analista tester realiza todas las pruebas pertinentes aplicando los filtros de testeo funcionales y no funcionales, bajo un mecanismo estandarizado y aprobado por SysCafé, el cual una vez terminado no se encuentra que correctamente aplicado, posteriormente se procede con el estado "Rechazado" al funcionario del área de desarrollo para su correspondiente corrección.

6.4Intercambio de Información

6.4.1 Política de intercambio de la información

El intercambio de información debe asegurar la confidencialidad e integridad de esta tanto al interior de la organización como externamente. Para garantizar la seguridad en el intercambio se tienen establecidas las reglas de distribución, receptores autorizados y medios de transferencia. Los controles de intercambio según la clasificación se describen a continuación:

Acceso	En medio físico	Intercambio electrónico	Medios de almacenamiento electrónico	Telefónico / fax
Pública	Sin restricción de intercambio.	Sin restricción de intercambio.	Sin restricción de intercambio.	Sin restricción de intercambio.
Uso Interno	Sobre sellado en mensajería normal.	Servicio de correo de la organización (no por correo remoto)	Control de envío bajo responsabilidad del propietario.	Se permite bajo responsabilidad del propietario.

Confidencial	Sobre sellado con control de envío y mensajería normal.	Servicio de correo de la organización identificado como seguro.	Registro de Control de envío de medios.	Se permite desde líneas telefónicas aprobadas y con las precauciones del usuario.
Secreta	Sobre sellado con mensajería especializada con acuerdo de seguridad.	Servicio de correo de la organización identificado como confidencial con la Información encriptada.	Registro de Control de envío de medios. Información protegida con clave. Información encriptado. Mensajería con acuerdo de seguridad.	No se acepta.

En caso de intercambio de información con partes externas (clientes, proveedores u otros) las reglas de este se definen en el Acuerdo de confidencialidad.

6.4.2 Acuerdos para el intercambio de información

El intercambio de información con partes externas en medios físicos solo se puede hacer por los servicios de mensajería aprobados por la dirección administrativa según el Proceso de Gestión Administrativa, Contable y Financiera y con los cuales se tiene establecido el acuerdo de confidencialidad. Las reglas para el intercambio de información con partes internas y externas son:

Acceso	Emisor	Receptor
Pública	Sin restricción de intercambio	Sin restricción de intercambio
Uso Interno	Puede hacer intercambio bajo responsabilidad del propietario y considerando los posibles riesgos.	Puede hacer intercambio bajo responsabilidad del propietario manteniendo un listado de receptores autorizados.

Confidencial	Se requiere autorización del líder de proceso.	Se requiere autorización del líder de proceso y listado de receptores autorizados.
Secreta	Se requiere autorización del líder de proceso.	Se requiere autorización del líder de proceso, listado de receptores autorizados y acuerdo de confidencialidad del receptor.

6.4.3 Reglas para intercambio de información según el medio

La información debe enviarse considerando los niveles de seguridad establecidos, aplicando los controles a continuación:

Medio	Empaquetado	Identificación y Etiquetado	Medio de Transporte	Otras reglas de uso
Correo en medio físico	Sobre sellado o caja de cartón que oculte contenido. El empaque debe ser tal que evite daño o deterioro	Identificación de la organización y remitente en el sobre y letra código del nivel de acceso (para documentación confidencial)	Empresa de mensajería aprobada por área administrativa y con acuerdo de confidencialidad. Servicio interno de mensajería	Información confidencial y secreta debe entregarse personalmente
Correo de medios de almacenamiento (USB, CD)	Sobre sellado o caja de cartón que oculte contenido. El empaque debe ser tal que evite daño o deterioro del medio.	Identificación de la organización y remitente en el sobre y letra código del nivel de acceso (para documentación confidencial)	Empresa de mensajería aprobada por área administrativa y con acuerdo de confidencialidad Servicio interno de mensajería	Información confidencial y secreta debe entregarse personalmente

Medio	Empaquetado	Identificación y Etiquetado	Medio de Transporte	Otras reglas de uso
Intercambio electrónico	N/A	El mensaje debe contener: Remitente. Cargo. Organización. y Nota de Confidencialidad en la firma	Servicio interno de mensajería electrónica y correo. No se permite uso de correo remoto.	Se aplican los procedimientos de uso de los servicios de procesamiento de información
Telefonía fija	N/A	N/A	Proveedor de servicios de telefonía aprobado	En lo posible evitar para información confidencial y no dejar mensajes con información sensible en contestador automático

El envío de la información se debe realizar a través del área administrativa.

6.5 Control Criptográfico

De forma general el control criptográfico aplica para el caso de transferencia de información confidencial o secreta por ser del cliente, estratégica o por requisitos legales.

SYSCAFÉ realiza la gestión de llaves de encriptación para generar certificados digitales a través de autoridades certificadoras para implementar acceso seguro a servidores web, certificar autenticidad en la instalación de las aplicaciones desarrolladas por **SYSCAFÉ** etc.

6.6 Copiado

6.6.1 Copias autorizadas

La autorización de copia de la información se determina en función del nivel de acceso y considerando el procedimiento de control de documentos y registros del sistema de gestión. La autorización de copias según el nivel de acceso se describe a continuación:

Acceso	Copias autorizadas
Pública	No se requiere autorización de copias.
Uso Interno	Pueden hacerse copias bajo responsabilidad del propietario, considerando los posibles riesgos y el procedimiento de control de documentos y registros.
Confidencial	Se requiere autorización del líder de proceso.
Secreta	Se requiere autorización del líder de proceso.

6.6.2 Consideraciones para copiado

El servicio de copiado debe ser tal que prevenga los riesgos de seguridad de la información, dado que la tecnología disponible de copiadoras aumenta las vulnerabilidades de seguridad. El término copiadora se refiere a:

- Máquinas fotocopiadoras.
- Impresoras
- Fax que producen salida impresa copia permanente.
- Pizarras electrónicas que proporcionan la reproducción de lo que está escrito en la tabla, y cualquier máquina con una combinación de estas funciones.

Los riesgos para considerar incluyen individuos que pueden intentar hacer copias desautorizadas de información, el mal uso de copiadoras por personas autorizadas; y riesgo técnico de la retención de información por imágenes latentes o residuales en las máquinas o memoria electrónica. Los controles de copiado incluyen:

- Documentos clasificados como confidenciales o secretos solo pueden copiarse con autorización de la dirección.
- Solo se debe hacer uso autorizado de los equipos de copiado para las personas del área o departamento. Para uso por externos se requiere autorización.
- La ubicación física de las copiadoras debe impedir el acceso no autorizado y deben estar lejos de áreas de tráfico altas donde personas desautorizadas tengan acceso.
- La compra de máquinas o equipos de copiado debe ser autorizada por el área técnica según los riesgos de seguridad. Solo se pueden hacer copias en horario laboral.

6.7 Almacenamiento y Manejo

Las directrices para el almacenamiento de información son:

- El almacenamiento de la información debe asegurar el control de acceso, preservación y disponibilidad de la información.

- La responsabilidad por el almacenamiento es directamente del propietario de la información o activo.

- Cada área o proceso de la organización debe disponer de un sitio de almacenamiento apropiado para la información confidencial o secreta con restricción de acceso físico mediante cerraduras u otras opciones tecnológicas apropiadas.

- Información confidencial o secreta no debe quedar en ninguna circunstancia sin protección de acceso.

- La información confidencial o secreta debe ser entregada solamente a personas que tengan la autorización apropiada.

- Si alguien requiere tener acceso a información confidencial como la Historia Laboral de los empleados, contratos, ésta debe ser consultada en compañía de la persona autorizada.

- El propietario de la información confidencial o secreta debe asegurar que las personas que no poseen una seguridad apropiada no tomen, lean, oigan por casualidad conversaciones o tengan acceso visual a la información confidencial o secreta.

- La información confidencial o secreta no debe estar situada o mostrada en cierto sentido donde se genere riesgo.

- La información confidencial o secreta debe discutirse sólo con esos individuos que poseen la autorización apropiada y no será discutida en público u otros lugares donde personas desautorizadas pudieran oír por casualidad.

- La información secreta no debe llevarse a una residencia privada, ni ser abierta, leída, mostrada o usada en vehículos, hotel, habitaciones y caja fuerte, avión, bus, cajones públicos, u otras localizaciones donde la información pueda transigir.

- Los puntos de almacenamiento de información confidencial o secreta deben estar provistos de controles adicionales al acceso como alarmas.

- El préstamo interno de los activos se controla mediante las planillas propias de cada área, bajo la supervisión del funcionario encargado de esta tarea. En los casos de préstamo externo, se elabora un acta de salida con la supervisión del Grupo de Infraestructura y previa autorización del área Administrativa.

- Si el control de acceso usa una clave se aplican las recomendaciones para uso de claves y contraseñas según el Procedimiento de Control de Acceso y Seguridad de Redes.

6.8 Destrucción de la información

La destrucción de la información debe considerar los tiempos de retención del activo según La Tabla de Retención Documental de la entidad, siguiendo además el Proceso de Disposición Final de los Documentos, establecido en el Programa de Gestión Documental de **SysCafé**.

De acuerdo con lo anterior, la destrucción debe ser tal que no permita la reconstrucción de la información. Para cada medio en el que se puede presentar la información las directrices de destrucción incluyen:

Medio	Método de destrucción	Autorización	Responsable
Medio físico (papel)	Máquina trituradora	Líder de proceso	Personal del proceso

Medios de almacenamiento (USB, CD)	Borrado y destrucción del medio	Líder de proceso	Administrador de Infraestructura Tecnológica
Electrónico	Borrado	Líder de proceso	Administrador de Infraestructura Tecnológica

La destrucción de información debe hacerse según sea necesario bajo los siguientes lineamientos:

- Entrega de equipos al proveedor o cliente.
- Tiempo de retención del activo agotado.
- Solicitud de la alta dirección.
- Requerimientos de ley según habeas Data, por solicitud del titular, limitado a su información.

6.9 Copias de Seguridad

Se realizan de acuerdo con el Procedimiento de Copias de Seguridad.

7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS						
N° Versión	Fecha de cambio			Descripción de cambios	Numeral(es)	Responsable
	Mes	Dia	Año			
1	06	30	2020	Versión inicial del procedimiento	Todo el documento	José Omar Mayorga Pabón, Gerente General
2	01	23	2023	Actualización de Alcance	2	Jorge Armando Varela Rendón, Asesor en Gestión Documental
3	01	09	2024	Actualización Documento	Todo el documento	Diana Karime Cruz Celis