1. OBJETIVO

Establecer las políticas y procedimientos para asegurar la utilización segura de la red y los servicios de procesamiento de información por parte de empleados, visitantes, contratistas y clientes.

2. ALCANCE

Incluirá la implementación de medidas de seguridad y controles de acceso para todos los sistemas de red y aplicaciones de la organización. Este procedimiento se aplicará a todos los usuarios internos y externos que tengan acceso a dichos sistemas y aplicaciones. Se incluirán medidas de seguridad tales como autenticación de usuario, encriptación de datos, cortafuegos, monitoreo de acceso y políticas de contraseña.

3. RESPONSABILIDAD

- Director de Seguridad de la Información
- Administrador de Seguridad de la Información
- Grupo de Infraestructura Tecnológica

4. TÉRMINOS Y DEFINICIONES

Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.

5. POLÍTICAS

- El uso de la red y los servicios de procesamiento de información, deben asegurar el acceso autorizado de empleados y contratistas, y evitar conexiones que pongan en riesgo la confidencialidad e integridad de la información, datos y servicios. Los controles de seguridad en la red se determinan con base en los resultados del proceso de gestión de riesgos.

- Este proceso aplica para el diseño y configuración de la red, creación y registro de usuarios en los sistemas de procesamiento, creación y revisión de derechos de acceso, conexión y uso de la red y retiro de derechos y privilegios en el sistema.

- Este proceso aplica para red de área local (LAN), red WAN, Internet, conexiones inalámbricas (Wireless), servicios de acceso remoto (VPN) y extranet.

- Este proceso aplica para nuevos servicios de procesamiento de la información, los cuales deben ser debidamente planeados y autorizados por la dirección.

- Los controles de seguridad en la red deben asegurar la protección de los recursos y la información con que se cuenta en la red, sin entorpecer los procesos de la organización. La responsabilidad directa por la seguridad de la red es del grupo de infraestructura, sin embargo, todos los empleados y contratistas tienen la responsabilidad por la aplicación.

6. DESCRIPCIÓN GENERAL

Para el control de acceso y seguridad en las redes, se llevan a cabo las siguientes actividades:

- Planeación y diseño de la red.
- Adquisición de Bienes y/o Servicios.
- Gestión de nuevos servicios de procesamiento.
- Prevención de ataques a la red.
- Acceso a los servicios de IT.
- Monitoreo del desempeño y seguridad de la red.

6.1 Planeación y diseño de la red

El **Director SI y el Grupo de Infraestructura Tecnológica** hacen el diseño y configuración de la red iniciando con la evaluación de las necesidades, considerando los objetivos de la organización y las necesidades de los procesos. Para este análisis se tiene en cuenta lo siguiente:

- Análisis del plan estratégico.
- Proyecciones de la demanda de tráfico.
- Análisis de la capacidad actual (monitoreo de uso y tráfico).
- Incidentes.
- Presupuestos.
- Análisis de riesgos.
- Cambios en los sistemas de información.

De acuerdo con las necesidades identificadas y las proyecciones se define o ajusta la topología de la red. El diseño de la topología consiste en seleccionar la estructura a utilizar incluyendo:

- Tipo.
- Equipos y tecnología.
- Fronteras, Routers y los firewalls.
- Segregación de funciones entre máquinas y separación de redes.
- Conexiones con terceros.
- Requisitos de tráfico para los niveles de servicio.

El diseño de la red debe garantizar la seguridad y controles definidos en la política de seguridad, el diseño de la red está en un diagrama.

6.2 Adquisición de Bienes y/o Servicios

Luego de identificar la tecnología apropiada para la red y compararla con la estructura actual y la disponibilidad de presupuesto, si es necesario algún recurso, el **Director SI** procede a adquirirla según los lineamientos de este proceso.
Si para el nuevo servicio de procesamiento de información se requieren recursos también se sigue este Proceso Gestión Administrativa y Financiera.

6.3 Gestión de nuevos servicios de procesamiento

Los servicios nuevos como la inclusión de un nuevo centro de datos deberían tener la autorización de la dirección. En este caso el **Grupo de Equipo de Infraestructura** será el encargado.
Se debe asignar un responsable del nuevo servicio de procesamiento con el fin de garantizar que se apliquen todas la políticas y requisitos de seguridad.
Si existe hardware y software para el nuevo centro de datos, este debe ser verificado antes de ser integrado al sistema.

6.4 Prevención de ataques a la red

Se llevan a cabo las siguientes actividades:

- Identificación de amenazas a la red y los sistemas de información.
- Selección de medios de control.
- Implementación de controles de seguridad.
- Concientización de usuarios.

6.4.1 Identificación de amenazas a la red y los sistemas de información

El **Coordinador de la Infraestructura Tecnológica** identifica las amenazas a la red y los sistemas de procesamiento de información teniendo en cuenta:

- El análisis de riesgos de los procesos.
- Las notificaciones de amenazas suministradas por los proveedores de productos y servicios de seguridad.
- Notificaciones de alertas de seguridad del sistema operativo.
- Auditorías externas.
- Eventos e incidentes de seguridad.
- Configuración de reglas de firewall en FORTINET

El **Director de SI** o el **Coordinador de Infraestructura Tecnológica** supervisan de forma constante el Router FORTINET, asegurando así su buen funcionamiento, ya que este monitorea diversas fuentes de amenazas.

Algunas de estas amenazas identificadas en la red pueden generar un evento de seguridad, debilidad de la Seguridad de la Información que incluso pueden generar un incidente de seguridad si ya se ha materializado.

6.4.2 Selección de medios de control

Según las amenazas identificadas y los resultados del comportamiento de la red, el **Coordinador de Infraestructura Tecnológica** define las herramientas apropiadas para la protección de los sistemas de información y las actividades que deben llevarse a cabo. Se debe evaluar, según el ataque de seguridad y las acciones que deben establecerse, si es necesario generar una acción correctiva, preventiva o de mejora.

6.4.3 Implementación de controles de seguridad

El **Coordinador de Infraestructura Tecnológica** implementa los controles establecidos que pueden incluir una herramienta o software de seguridad. Se llevan a cabo las acciones establecidas para el tratamiento de la amenaza.

6.4.4 Concientización de usuarios

Como una importante medida de control el **Director de SI** realiza un proceso de concientización de los usuarios en los riesgos de seguridad asociados a ataques por códigos maliciosos y móviles. Esta concientización se apoya en el **documento Manual de Políticas de Seguridad de la Información.**

6.5 Acceso a los servicios de IT

Las actividades que se llevan a cabo se describen a continuación:

- Solicitud de acceso y privilegios.
- Verificación de derechos de usuario.
- Definición de privilegios y accesos.
- Notificación de accesos.
- Monitoreo de derechos de acceso y privilegios.

6.5.1 Solicitud de acceso y privilegios

La solicitud de acceso y privilegios a los servicios del procesamiento de información se realiza en los siguientes casos:

- Contratación de personal.
- Contratación de servicios que requieran la conexión a los servicios de procesamiento.
- Cambios organizacionales.
- Asignación de un rol o proyecto nuevos.

Cuando se presentan alguno de estos casos la Dirección Administrativa o del área responsable hacen la solicitud al **Grupo de Infraestructura Tecnológica** por medio de la herramienta GLPI.

6.5.2 Verificación de derechos de usuario

El **Coordinador de Infraestructura Tecnológica** verifica las políticas para acceso a la información y a los servicios de IT, relacionados con el rol y los derechos de acceso. Esto incluye tanto los derechos de nuevos usuarios como el cambio de privilegios de usuarios ya existentes.

6.5.3 Definición de privilegios y accesos

Si los accesos son aprobados, el **Coordinador de Infraestructura Tecnológica** define los privilegios y accesos de la siguiente manera:
Si el usuario no existe, se crea el usuario en la red definiendo: identificación y contraseña, siguiendo los lineamientos del Procedimiento de Administración de Usuarios y Contraseñas para el uso de contraseñas y posteriormente se definen los accesos a servicios de IT y Bases de datos.
Para usuarios ya existentes, se revisan los privilegios actuales y se definen los accesos solicitados.
La asignación de accesos debe considerar los requisitos de seguridad y la política de control de acceso. Según el Manual de Políticas de Seguridad de la Información.
Para garantizar que los usuarios no tengan cuentas redundantes se hace revisión de los Id en el Directorio Activo.
El acceso al sistema de información lo define el responsable de cada sistema y se hace a través del módulo de seguridad que ofrezca la aplicación.
Se definen los accesos a los respectivos servicios de IT, de acuerdo con las solicitudes realizadas.

El acceso a códigos fuente de los programas se restringe mediante la autorización de personal el cual solo es otorgado únicamente al personal del área de desarrollo de proyectos, se usa la herramienta DEVOPS ya que con ella se permite tener un repositorio de los proyectos de SysCafé, a su vez con el servidor de programación.

6.5.4 Notificación de accesos

Mediante un correo interno y respuesta de la solicitud escalada a la mesa de ayuda GLPI, el **Coordinador de IT** notifica a quien realiza la solicitud los accesos definidos.
Las condiciones relacionadas con los derechos de acceso son aprobadas por el usuario con la firma o renovación del acuerdo de confidencialidad como se establece en el Proceso de Gestión de Talento Humano.

6.5.5 Monitoreo de derechos de acceso y privilegios

El **Coordinador de Infraestructura Tecnológica** hace monitoreo mensual sobre el vencimiento de los accesos y privilegios asignados, de acuerdo con los reportes de retiro solicitados por la Gerencia General o la Dirección Administrativa. El retiro de acceso y privilegios a los servicios del procesamiento de información se realiza en los siguientes casos:

- Terminación de contrato del personal
- Terminación de contratación de servicios que requieran la conexión a los servicios de procesamiento.
- Cambios en los sistemas de procesamiento.

Cuando se presentan alguno de estos casos, la Dirección Administrativa notifica mediante una solicitud a la mesa de ayuda GLPI, al **Coordinador de Infraestructura Tecnológica** para proceder a eliminar el ID y retirar privilegios en este caso, se debe notificar al cliente o proveedor que preste servicios al empleado para que retire los accesos pertinentes.

6.5.6 Consideraciones generales para los medios accesos a los servicios IT

Redes Inalámbricas

En SysCafé actualmente se tiene implementado el acceso a Internet wifi el cual se encuentra totalmente aislado de la red corporativa, de forma física y lógica. Este se utiliza sólo cuando se requiere dar acceso a algún invitado que requiere acceso a Internet, pero no a la red corporativa.

Bases de Datos

En **SYSCAFE** se utilizan motores de base de datos de SQL Server en la versión 2019.
Los ambientes se encuentran separados para los diferentes proyectos y para los diferentes roles, es decir, el ambiente de desarrollo está separado del ambiente de pruebas, aceptación y producción.
En algunos casos, cuando el proyecto, la aplicación, o la configuración lo requiera, se asigna una instancia de base de datos independiente.
La autenticación de base de datos se hace según los requerimientos del proyecto ya sea por autenticación en el Directorio Activo o autenticación con usuarios de la base de datos.

Puertos de Configuración

El acceso lógico y físico a los puertos de configuración de los servidores y de los equipos de red principales está controlado.
Los controles para el acceso físico incluyen la restricción de acceso físico al centro de cómputo, solo tienen acceso el personal de infraestructura.
El acceso lógico se controla con claves de acceso y protocolos de administración remota seguros y disponibles solo al personal de infraestructura encargados de dichas tareas y solo desde las instalaciones de la compañía.
Los puertos de los servidores y equipos de red están, por defecto, cerrados y se abren los que sean necesarios para prestar los diferentes servicios de red.

6.6 Monitoreo del desempeño y seguridad de la red

Para asegurar el correcto funcionamiento de la red y servicios de procesamiento de información, el **Coordinador de Infraestructura Tecnológica** ejecuta las siguientes actividades de monitoreo:

- Monitoreo de estado de servicios.

- Monitoreo de eventos y accesos.
- Monitoreo de Códigos maliciosos
- Monitoreo de actualizaciones.
- Administración de Incidentes de Seguridad.

6.6.1 Monitoreo de estado de servicios

El **Coordinador de IT** monitorea el estado de los servidores y los servicios que utiliza. Si se presenta alguna inconsistencia, esta es reportada por correo al responsable del servicio.

6.6.2 Control de eventos y accesos

El **Coordinador de Infraestructura Tecnológica** controla el funcionamiento adecuado de la herramienta con base a los reportes detectados por los usuarios y en lo detectado en los mantenimientos planeados.

6.6.3 Monitoreo de Códigos maliciosos

El **Coordinador de Infraestructura Tecnológica** monitorea los virus reportados, spam, máquinas infectadas. (determinar, actuar)

6.6.4 Monitoreo de Actualizaciones

El monitoreo de actualizaciones también puede ayudar a prevenir problemas de compatibilidad, ya que los desarrolladores a menudo emiten actualizaciones para abordar estos problemas. En general, el monitoreo de actualizaciones es una práctica importante para garantizar la seguridad y el rendimiento óptimo de los sistemas tecnológicos.

6.6.5 Administración de Incidentes de Seguridad

Si alguna de las actividades de monitoreo representa un incidente de seguridad, un evento o una debilidad, El **Coordinador de Infraestructura Tecnológica** la reporta siguiendo los lineamientos del Procedimiento Gestión de Incidentes.

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 objetivo y alcance Eliminación de documentos relacionados Se complementa numeral 6.6.4	1,2 y 6.6.4	Fabian Barco
3	01	09	2024	Actualización Documento	Todo el documento	Diana Karime Cruz Celis
4	11	12	2024	Actualización Documento	Todo el documento	Diana Karime Cruz Celis