2023

CARTILLA INSTRUCTIVA INGEURBANISMO SAS

SISTEMA TECNOLOGICO DE RESTRICCIÓN A REDES SOCIALES EN HORARIO LABORAL Y MEJORAR PRODUCTIVIDAD.

La presente cartilla se presenta como una guía donde se comunica el proceso diseñado respecto al sistema tecnológico para bloquear las redes sociales a los trabajadores de la compañía durante el horario laboral y con ello mejorar su rendimiento.

TABLA DE CONTENIDO

INTRODUCCIÒN

USO DE REDES SOCIALES EN HORARIO LABORAL AFECTA LA PRODUCTIVIDAD

La compañía INGEURBANISMO SAS es una empresa que desarrolla sus servicios en el sector constructivo y se encuentra ubicada en la ciudad de Rionegro, Antioquia

La compañía cuanta con una oficina principal cuya planta administrativa esta conformada por 40 trabajadores y tienen destinados 40 computadores cada uno.

La compañía identifico la problemática presentada con el uso de las redes sociales por parte de sus trabajadores durante el horario laboral, que ocasionaba un bajo rendimiento.

En atención a lo anterior, la compañía solicito un solución que permitiera restringir o bloquear el acceso a las redes sociales en la jornada laboral y con ello mejorar el rendimiento de los trabajadores.

Por lo anterior, se diseño como solución un sistema tecnológico que permite atender la problemática identificada e informada por la compañía, la cual se desarrolla en esta Guía.

PROBLEMA Y SOLUCIÓN

PROBLEMA:

La compañía mediante una investigación desarrollada, logro identificar un bajo desempeño de sus trabajadores causado por el uso de las redes sociales durante el horario laboral.

lo anterior ha presentado dificultad en la compañía para poder restringir a bloquear el uso de las redes sociales y de esta forma evitar que sus trabajadores se distraigan en otras actividades.

SOLUCIÓN:

se presenta un sistema tecnológico que permite realizar un control, restricción o bloqueo respecto al uso de las redes sociales por parte de los trabajadores en su horario Laboral. logrando consigo mejorar la productividad en los trabajadores de la compañía.

" CONCÉNTRATE EN LO PRODUCTIVO NO EN ESTAR OCUPADO
TIM FERRISS

SISTEMA TECNOLOGICO

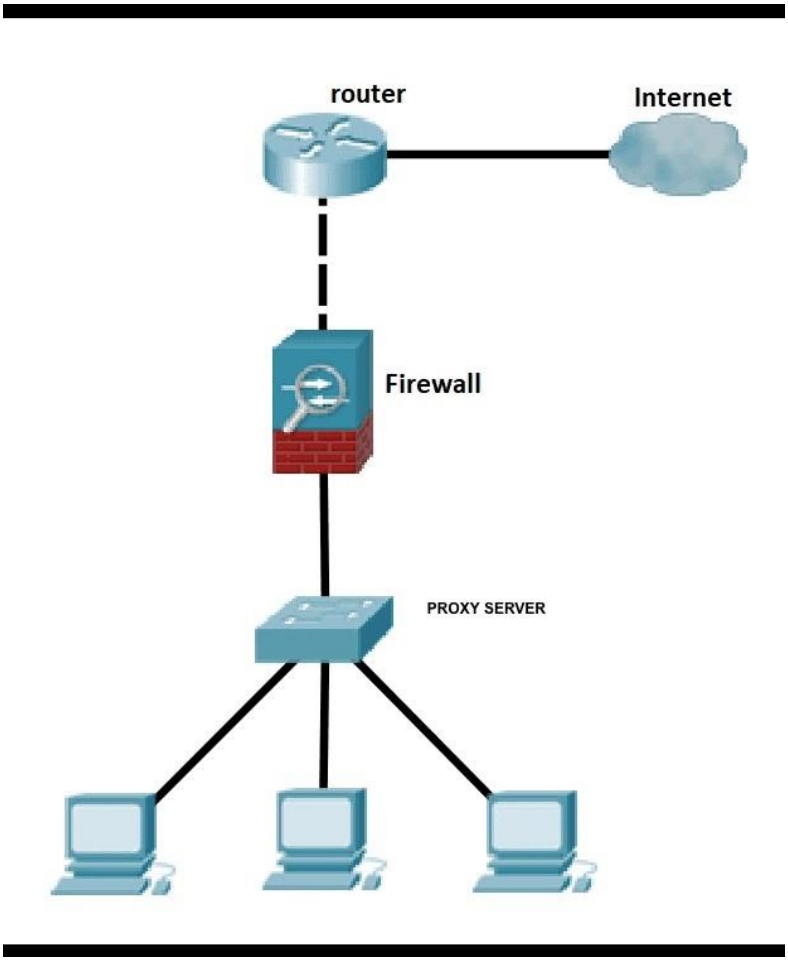
El sistema tecnológico, está conformado por tres herramientas tecnológicas que son:

- Router Cisco ISR.
- Firewall
- Proxy

Las herramientas mencionadas actúan simultáneamente para restringir o bloquear el acceso a las redes sociales por parte de los trabajadores de la compañía durante su jornada laboral.

Igualmente, el presente sistema también brinda una protección a la seguridad informática de la compañía al bloquear y restringir sitios web peligrosos o de descargas de archivos malignos.

Posteriormente, después de haber realizado por determinado tiempo establecido por la compañía, la restricción o bloqueo a los trabajadores a las redes sociales durante el horario laboral, se podría observar las mejoras en la productividad de los trabajadores.



CAPACITACIÓN

El procedimiento para capacitar a los trabajadores de la empresa en el uso del sistema técnico de bloqueo compuesto, puede seguir los siguientes pasos:

1.- Planificación de la capacitación: Establecer mínimo una periodicidad de 2 veces al año para efectuar las capacitaciones.

2.- Preparación del material: Material de capacitación que incluya información sobre el sistema técnico de bloqueo, sus funciones, ventajas y el procedimiento para bloquear páginas de redes sociales. Esto puede incluir presentaciones, manuales o guías de referencia.

3.- Comunicación previa: Informar a los trabajadores sobre el problema de bajo rendimiento causado por el uso de las redes sociales durante el horario laboral, los daños y perjuicios que ocasionan dichas practicas. Igualmente informar a los trabajadores las medidas que va a implementar la compañía respecto al bloqueo o restricción de dichas redes sociales mediante el sistema tecnológico propuesto.

l4.- Normatividad. Informar a los trabajadores de la compañía los argumentos jurídicos que permiten a la compañía aplicar el sistema tecnológico.

5.- Explicación del sistema: en este punto se exponen los conceptos de las herramientas tecnológicas utilizados por el sistema, tales como router, firewall y proxy; como también sus funciones y características.

6.- Práctica y ejercicios: Proporcionar oportunidades para que los trabajadores experimenten un bloqueo o restricción de redes sociales en horario laboral.

PASO 1. CONFIGURACIÓN ROUTER.

INICIAR CON LOS PASOS GENERALES:

1.- Identificar los requisitos específicos de bloqueo de páginas web de redes sociales. Esto implica determinar qué sitios web de redes sociales se bloquearán y qué criterios se utilizarán para el bloqueo, como URLs, palabras clave, categorías, etc.

2.- Acceder a la interfaz de configuración del Router Cisco ISR utilizando un navegador web y las credenciales de administrador correspondientes.

3.- Configurar una lista de acceso (ACL) que defina las reglas para el bloqueo de las páginas web de redes sociales. Esto implica establecer reglas que denieguen el acceso a los sitios web específicos o las categorías relacionadas.

4.- Aplicar la ACL a la interfaz o interfaces correspondientes del Router Cisco ISR. Esto permitirá que el enrutador inspeccione y filtre el tráfico que pasa a través de esas interfaces.

5.- Realizar pruebas de funcionamiento para verificar que el bloqueo de las páginas web de redes sociales esté funcionando correctamente. Esto puede incluir intentar acceder a los sitios web bloqueados desde una computadora de la red y confirmar que se muestre un mensaje de bloqueo o se impida el acceso.

CONTINUAR CON LOS PASOS ESPECIFICOS:

1.- Accede al router: Conéctate al router Cisco mediante un cable de consola o a través de una conexión de red.

2.-Ingresa al modo de configuración: Una vez conectado, ingresa al modo de configuración del router. Puedes hacerlo utilizando el comando `*enable*` seguido de la contraseña de privilegio.

3.- Configura la interfaz de salida: Identifica la interfaz a través de la cual se enviará el tráfico hacia Internet y configúrala. Puedes utilizar el comando `*interface <nombre de la interfaz>*` para seleccionar la interfaz y luego configurar la dirección IP correspondiente.

4.-Crea una lista de acceso: Utiliza el comando `*access-list <número de lista> <permit|deny> <dirección IP o rango> <wildcard>*` para crear una lista de acceso. En este caso, debes utilizar el comando `*deny*` para bloquear las direcciones IP o rangos correspondientes a las páginas web que deseas bloquear. Puedes encontrar información detallada sobre cómo especificar las direcciones IP o rangos en la documentación de Cisco.

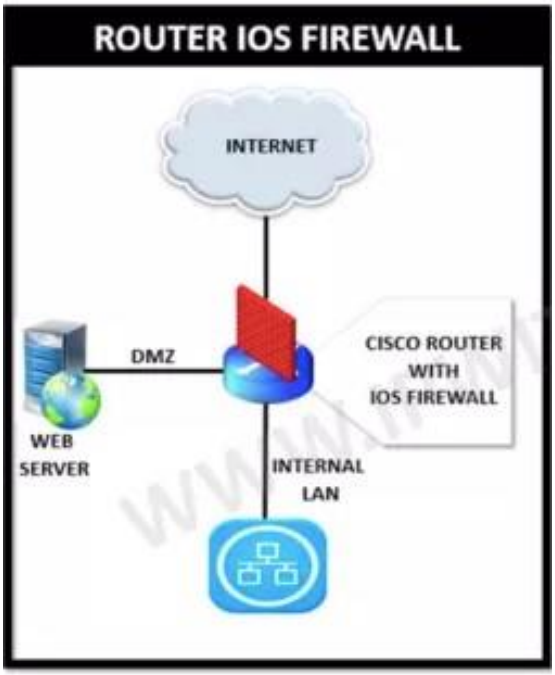
5.- Aplica la lista de acceso a la interfaz: Utiliza el comando `*ip access-group <número de lista> <in|out>*` para aplicar la lista de acceso creada en el paso anterior a la interfaz de salida. Elige el parámetro `*out*` si deseas bloquear el tráfico saliente hacia las páginas web, o elige *´in´* si deseas bloquear el tráfico entrante desde esas páginas web.

6.- Guarda la configuración: Utiliza el comando `write memory` o `copy running-config startup-config` para guardar la configuración realizada en el router.

PASO 2. CONFIGURACIÓN FIREWALL.

Se instalaría y configuraría un firewall que permita establecer políticas de seguridad y reglas de acceso. En este caso, se definirían reglas específicas para bloquear el tráfico relacionado con las redes sociales como Facebook, WhatsApp, Instagram y TikTok entre otras definidas por la compañía. Esto se lograría mediante la configuración de reglas de filtrado basadas en direcciones IP, puertos y protocolos utilizados por estas plataformas.

2.1.- Identificar las páginas web de redes sociales que se desean bloquear y crear una lista de direcciones URL.



2.2.- Configurar el firewall para bloquear el tráfico de estas direcciones URL.

2.3.- Establecer reglas de filtrado de contenido para bloquear cualquier contenido relacionado con las páginas de redes sociales que no estén en la lista de direcciones URL bloqueadas.

2.4.- Establecer políticas de seguridad para garantizar que los empleados no puedan evitar el bloqueo utilizando proxies o herramientas similares.

2.5.- Probar el firewall para asegurarse de que está bloqueando adecuadamente las páginas de redes sociales seleccionadas.

2.6.- Realizar ajustes en la configuración del firewall según sea necesario para garantizar un bloqueo efectivo de las páginas de redes sociales.

PASO 3. CONFIGURACIÓN PROXY.

Se establecería un proxy como intermediario entre los usuarios y los servicios en Internet. El proxy permitiría filtrar y controlar el tráfico web, bloqueando el acceso a los sitios y servicios específicos de las redes sociales objetivo. Se configurarían reglas para bloquear el acceso a los dominios y direcciones IP asociadas con Facebook, WhatsApp, Instagram TikTok y demás redes sociales determinadas por la compañía.

1.-Se deben configurar las reglas del software proxy para bloquear las páginas web de redes sociales y permitir únicamente el acceso a los sitios web permitidos por la empresa.

2.- Accede al modo de configuración del router. Esto se puede hacer a través de la interfaz de línea de comandos (CLI) utilizando un programa de emulación de terminal como PuTTY.

3.- Configura la interfaz del router que se utilizará como interfaz de salida para el tráfico del proxy. Por ejemplo, supongamos que la interfaz FastEthernet0/0 será utilizada. Puedes usar el siguiente comando para configurar la interfaz:

interface FastEthernet0/0
ip address [dirección_IP_del_router] [máscara_de_red]

4.- Configura el servidor proxy. Puedes utilizar el siguiente comando para configurar el servidor proxy en el router:

ip http server

5.- Configura el filtrado de URL. Utiliza el siguiente comando para definir la lista de sitios web que deseas bloquear:

ip urlfilter [acl_number] block url [url_pattern]

Donde:

- [acl_number] es el número de lista de acceso que se utilizará para el filtrado.
- [url_pattern] es la expresión regular o el patrón de URL que se bloqueará. Por ejemplo, puedes usar ".facebook.com." para bloquear cualquier URL que contenga "facebook.com".

6.- Aplica la lista de acceso al tráfico saliente. Utiliza el siguiente comando para aplicar la lista de acceso de filtrado de URL a la interfaz de salida:

access-list [acl_number] deny any any

7.- Configura la ruta predeterminada. Puedes usar el siguiente comando para configurar la ruta predeterminada para el tráfico que no esté bloqueado por el proxy:

ip route 0.0.0.0 0.0.0.0 [dirección_IP_del_gateway]

8.- guardar configuración y reiniciar el router para aplicar los cambios.

COSTOS DEL SISTEMA

El proyecto se desarrollará por el término de un año.

El presupuesto destinado por parte de la compañía para la implementación de la solución de sistema tecnológico presentado, es por valor de $8500 US.

Los costos directos son:
Router Cisco ISR 4000 Series Modelo ISR4321-V/K9
Firewall IOS Cisco
Proxy.

Los costos indirectos son:
Soporte técnico.

Los costos fijos:
Internet.

Los costos variables son:
Servicio público de energía.

Gastos Generales son:
Pago nómina individual del trabajador que operará el sistema.

Capital de trabajo:
Capacitación de personal de la compañía.

Valores dados con proyeccion a 1 año
Presupuesto del Proyecto $8.500 US
Servicio: SISTEMA TECNOLOGICO DE BLOQUEO

DESCRIPCIÓN	VALOR UNITARIO	UNIDADES	VALOR TOTAL	TIPOS DE COSTOS	FRECUENCIA
Router Cisco ISR 4000 Series Modelo ISR4321-V/K9	$ 3.300	1	$ 3.300	Directo	Unica
Firewall IOS Cisco	$ -	1	$ -	Directo	Unica
Proxy	$ 2	1	$ 24	Directo	Mensual
Soporte Tecnico	$ 100	1	$ 100	Indiecto	Anual
Internet	$ 50	1	$ 600	Fijo	Mensual
Servicio publico Energia	$ 1,33	1	$ 16	Variable	Mensual
Capacitación Personal Compañía	$ 50	1	$ 50	Fijo, gastos generales	Diario
Recurso humano operación y mantenmiento	$ 350	1	$ 4.200	Directo, Gastos gnerales	Mensual
Valor Total, entregados en dolares americanos			$ 8.290		

EL SISTEMA TECNOLÓGICO DISEÑADO PRESENTA UN AHORRO DE $210 US

ATENCIÓN Y GARANTIA DEL SERVICIO

Duración de la garantía: por seis (6) meses contados desde la fecha de implementación del sistema.

Cobertura de la garantía: la garantía comprende las herramientas de, El router, el firewall, el prox, mantenimiento del sistema.

Exclusiones de la garantía: cuando se presenten daños causados como el mal uso, negligencia, alteración no autorizada, indebida manipulación, desastres naturales u otras circunstancias fuera del control del prestador del servicio, de acuerdo a las condiciones de ley en la normatividad colombiana.

Procedimiento de reclamación: Se debe de notificar en un término máximo de tres días hábiles a la dirección de correo electrónico ebarney84674@universidadean.edu.co

Conmutador: (604) 6450012
Celular: 3112662888
Dirección: Carrera 15, #7-84, Sector Llano grande.
Correo electrónico: ebarney84674@universidadean.edu.co
Rionegro, Antioquia.