GOB-PT-019 Política de Seguridad en Redes V2

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

1. OBJETIVO

Establecer directrices de seguridad en las redes que permitan administrar y gestionar los recursos de conectividad de la Concesión RUNT 2.0, con el fin de proteger la información de los sistemas y aplicaciones que las usan.

2. ALCANCE

El alcance de la presente política abarca los controles de la NTC ISO/IEC 27002:2022 pertinentes para la Seguridad en Redes. Así mismo, se tendrán en cuenta la seguridad de los servicios de red, su segregación y el filtrado web que deberá ser aplicado en los diferentes componentes de la arquitectura de conectividad del sistema RUNT.

3. DIRECTRICES GENERALES DE LA POLITICA PARA LA SEGURIDAD EN REDES

Con el fin de proteger la información que transita por las redes, la Concesión RUNT 2.0 deberá:

a. Diseñar las redes para que los dispositivos estén separados en función de los niveles de confianza, criticidad y sensibilidad. Se deben separar de la red pública. El perímetro de cada red debe estar bien definido y contar con un dispositivo que controle el paso entre redes.

b. Identificar las responsabilidades y designar las personas que van a realizar gestión sobre los equipos y dispositivos en la red.

c. Mantener la documentación actualizada de las configuraciones de los equipos y dispositivos en la red, así como su arquitectura de detalle y diagramas de red indicando claramente el direccionamiento IP, nombre de la red y funcionalidad.

d. Cumplir con los controles asignados para proteger la información cuando se transmita por redes públicas o de terceros como por ejemplo con el uso de VPN, cifrado de la información, certificados, acuerdos de confidencialidad y seguridad para la transferencia de información, entre otros.

e. Monitorear regularmente los servicios de las redes con el fin de detectar posibles acciones que puedan afectar la seguridad, como por ejemplo la detección de comportamientos anómalos mediante herramientas, revisión de logs, verificación de accesos y permisos, etc. Dichos eventos se deben notificar a los canales definidos para la gestión de incidentes.

f. Restringir el acceso físico a los dispositivos de red solo al personal autorizado para su gestión.

g. Restringir y filtrar las conexiones de los sistemas de red, por ejemplo, usando políticas de firewall.

h. Separar los canales de administración de red de otros tráficos de la red.

i. Realizar una verificación de los protocolos y puertos utilizados para identificar y gestionar las posibles vulnerabilidades.

3.1. DIRECTRICES SOBRE LA SEGURIDAD DE LOS SERVICIOS DE RED

La Concesión RUNT 2.0 debe garantizar la seguridad en el uso de los servicios de red mediante su identificación y monitoreo. El uso de las redes y sus servicios deben implementarse teniendo en cuenta lo siguiente:

a. Los accesos definidos únicamente a redes y servicios permitidos

b. Los requisitos de autenticación y acceso para cada uno de los servicios en la red, teniendo en cuenta la política de contraseñas establecida en la Concesión RUNT 2.0.

c. Los medios por el cual se accede a la red, por ejemplo, si es por VPN o redes inalámbricas.

d. Monitorear el uso de los servicios de red por medio de los registros de logs.

e. Verificar la capacidad del proveedor de servicios de red para gestionar de forma segura los servicios acordados, por ejemplo, definiendo los niveles de servicio y haciendo seguimiento al cumplimiento.

f. Implementar dispositivos de seguridad que permitan el filtrado del tráfico (cortafuegos) entre las redes internas de Concesión RUNT 2.0 y las redes externas, tales como proveedores, clientes o conexiones internacionales con otras empresas.

g. Implementar dispositivos de detección de intrusos que permitan monitorear, detectar e impedir accesos no autorizados.

3.2. DIRECTRICES SOBRE LA SEGURIDAD PARA LA SEGREGACIÓN DE LAS REDES

Con el fin de controlar el tráfico que circula por las redes, la Concesión RUNT 2.0 deberá dividir las redes en límites de seguridad, logrando la segregación de los grupos de los servicios de información, usuarios y sistemas de información, teniendo en cuenta lo siguiente:

a. Dividir la red en segmentos separados aislándolos de la red pública (internet), esta división se puede realizar por niveles de confianza, criticidad, y sensibilidad, por ejemplo, red para el acceso al público, acceso interno, servidores, aplicaciones, etc, o por unidades organizativas, por ejemplo, gestión humana, financiera, comercial, etc.

b. Controlar el acceso a cada perímetro de red por ejemplo mediante una puerta de enlace por medio de un cortafuegos o un enrutador de filtrado. Este control de acceso debe estar alineado el GOB-PT-006 Política de Control de Accesos e Identidades de la Concesión RUNT 2.0.

c. Controlar de forma especial las redes inalámbricas debido a que pueden tener perímetros de red mal definidos, se debe ajustar la cobertura de radio para la correcta segregación de la red.

d. En el caso de tener entornos sensibles, se debe considerar los accesos inalámbricos como redes externas y la seguridad que conlleva, por ejemplo, segregar el acceso a la red interna hasta que haya pasado a través de una puerta de enlace (cortafuego).

e. La red inalámbrica de acceso a invitados debe separarse de la red interna y debe cumplir con la política GOB-PT-006 Política de Control de Accesos e Identidades de la Concesión RUNT 2.0.

3.3. DIRECTRICES SOBRE LA SEGURIDAD PARA EL FILTRADO WEB

Con el fin de evitar exposición a contenido malicioso en internet, la Concesión RUNT 2.0 debe administrar el acceso a este recurso teniendo en cuenta las siguientes directrices:

a. Se deben identificar los tipos de sitios web a los que el personal debería o no tener acceso. La organización debe bloquear el acceso a los siguientes tipos de sitios web:
   i. sitios web que tengan una función de carga de información a menos que se permita explícitamente por razones comerciales válidas;
   ii. sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen contenido de malware o phishing);
   iii. servidores de comando y control;
   iv. sitio web malicioso adquirido de inteligencia contra amenazas
   v. sitios web que comparten contenido ilegal
   vi. En general otros sitios que se consideren de comportamiento malicioso.
b. Reducir el riesgo para que el personal de la Concesión RUNT 2.0 acceda a sitios web que contengan información ilegal o maliciosa, esto se consigue bloqueando las IPs que se reportan por distintos medios como grupos de seguridad, mensajes de proveedores, entre otros.

c. Contar con protección antimalware como el antivirus que verifican la navegación.

3.4. DIRECTRICES SOBRE LAS CONEXIONES DE LOS OT y DT SOBRE SD-WAN

A continuación, se definen los lineamientos para las conexiones generadas al sistema RUNT por parte de los Organismos de Tránsito, Direcciones Territoriales y estaciones de trabajo del Ministerio de Transporte cuyo acceso será responsabilidad de la Concesión RUNT 2.0.

a. Cada dispositivo debe estar totalmente identificado, No deben utilizar direcciones genéricas o NATs. El objetivo es contar con la visibilidad individual de los equipos que están accediendo al sistema RUNT, para que en el caso de detectar

comportamiento malicioso de una IP se pueda bloquear individualmente y no se comprometan todas las máquinas.

b. El administrador responsable de cada IP con acceso debe estar identificado a través de un inventario del direccionamiento IP, donde estén registrados los datos de contacto en caso de un incidente. Este inventario debe ser actualizado con periodicidad mensual.

c. La cantidad de direcciones IP habilitadas para cada OT/DT debe guardar relación de proporcionalidad 2 a 1, de acuerdo con la cantidad de usuarios que cuenten con acceso al sistema RUNT.

d. Se debe mantener actualizado el inventario del direccionamiento IP y el tipo de dispositivo que hay conectado a cada dirección IP que tiene acceso al canal. Esto es: PC, impresora o router.

e. Los dispositivos que se conecten a través del canal SD-WAN deben tener acceso únicamente a los servicios que requieren para su función misional relacionada con el Registro Nacional de Tránsito.

f. Se debe definir y controlar el tráfico que se tiene por el canal SD-WAN, para que sea asignado en función de los sitios web autorizados que tengan relación con el cumplimiento de las condiciones Técnicas y Tecnológicas para la operación del sistema RUNT.

g. Dentro del ancho de banda del canal se debe prever la necesidad periódica de actualizar los PC y su software y programar las actualizaciones en horarios no hábiles. Se deberá asignar parte del ancho de banda a las actualizaciones y el resto a la operación para evitar eventos de saturación del canal por dichas actualizaciones. En estas actividades de actualizaciones periódicas tendrán especial prioridad las referentes a temas de seguridad que serán aplicadas según su criticidad.

h. Se debe monitorear el comportamiento de las conexiones, las estaciones y los usuarios. Ante posibles comportamientos maliciosos se debe notificar al responsable del dispositivo afectado para que haga la respectiva investigación, previo el corte preventivo del acceso de la máquina con dicho comportamiento.

4. CONTROL DE CAMBIOS

Control de cambios					
Versión	Elaboró	Revisó	Aprobó	Fecha	Descripción
1	IT Managers	Jefe Seguridad de la información	Líder de Seguridad de Información	21/07/2023	Creación del documento
2	Analista de seguridad de la información	Jefe Seguridad de la información	Jefe Seguridad de la información	19-04-2024	Se ajusta clasificación de la información.

Tabla 1. Control de cambios