NORMATIVA DE GESTIÓN DE ACCESO REMOTO

NOR-003

Descripción breve

Este documento describe la normativa que deben cumplir las personas usuarias del servicio de acceso remoto.

Con la financiación de la GENERALITAT VALENCIANA y FEDER

GENERALITAT VALENCIANA
Conselleria de Sanitat Universal i Salut Pública

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	03/06/2024	Responsable de Seguridad	Versión inicial del documento

Con la financiación de la GENERALITAT VALENCIANA y FEDER

Índice

1. OBJETO 4
2. ALCANCE 4
3. DEFINICIONES 4
4. DESARROLLO 5
4.1 Acceso individual por VPN 6
4.2 Acceso por LAN to LAN 7
4.3 Acceso de Proveedores 8
4.4 Acceso a documentos compartidos y trabajo colaborativo 8
5. COMUNICACIÓN DE DEFICIENCIAS DEL PROCEDIMIENTO 9
6. DOCUMENTACIÓN COMPLEMENTARIA 9
7. ANEXOS 9
7.1 Anexo- RECOMENDACIONES 9

Con la financiación de la GENERALITAT VALENCIANA y FEDER

1. OBJETO

El objeto de este procedimiento es recoger de forma integral las acciones a realizar en la gestión del acceso remoto del sistema.

Este documento se rige en definición, desarrollo y circuito de aprobación por la norma de Gestión de la documentación.

Cualquier posible incumplimiento de esta normativa, estará sujeto a lo dispuesto en el apartado Proceso Disciplinario de la Normativa de Uso de Medios Electrónicos.

2. ALCANCE

Todos los sistemas de información y el personal relacionado con el Centro de Investigación Príncipe Felipe.

3. DEFINICIONES

VPN: Una red privada virtual (RPV) (en inglés, Virtual Private Network, VPN) es una tecnología de red de ordenadores que permite mediante técnicas criptográficas, una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Segmentación de Red: Consiste en la división de una red en distintas subredes más pequeñas con el propósito de mejorar no solo el rendimiento global de la red, sino, sobre todo, sus condiciones de seguridad. La segmentación permite el control de tráfico entre las distintas subredes, en base a políticas definidas de segmentación, lo que aísla y mejora la seguridad.

Mitigar: Moderar, disminuir o suavizar algún parámetro o atributo, como puede ser el nivel de riesgo.

Cifrado: el cifrado es un procedimiento que emplea algún mecanismo criptográfico para proteger la confidencialidad y, en su caso, la integridad y la autenticidad de la información.

Acceso: es el resultado positivo de una autentificación.

4. DESARROLLO

La siguiente normativa pretende regular los principios generales de interconexión y acceso remoto a los sistemas de información del Centro de Investigación Príncipe Felipe, ofreciendo pautas y requerimientos mínimos que deben ser cumplidos respecto al uso de VPNs, así como redirigiendo al procedimiento adecuado respecto a las conexiones LAN to LAN con otras redes propias o ajenas.

Cada día la presencialidad para llevar a cabo una determinada tarea es menos necesaria, pudiendo ser ésta realizada por colaboradores localizados en diferentes ubicaciones, lo que implica necesariamente la necesidad de conceder permisos para el acceso remoto. Es evidente que estas modalidades no deben descuidar la seguridad y protección de la información, así como los datos de las organizaciones.

Se considerará acceso remoto al realizado desde fuera del perímetro de las propias instalaciones de la organización. Para llevar a cabo la autorización de acceso remoto es evidente que las organizaciones necesitan establecer normas, restricciones, procedimientos y mecanismos operativos que doten al acceso de la necesaria seguridad.

Para realizar la solicitud del acceso remoto, el interesado o su responsable deberá crear un ticket en el sistema de soporte del CIPF (https://soporte.cipf.es) con la categoría *"VPN"*, que deberá ser aprobado por el responsable de Seguridad, según se indica en el apartado correspondiente del Procedimiento de Gestión de Autorizaciones. La solicitud ha de ser clara y concreta, y puede referirse a un período de tiempo determinado para realizar determinadas tareas, o bien mientras dure la vinculación con la organización, como sería el caso de una situación contractual con un proveedor, un contrato laboral con personal interno, o la aceptación del destino de un funcionario público en una Organización perteneciente a dicho sector.

Los permisos de acceso remoto se darán de baja una vez se terminen las causas que motivaron la solicitud.

A continuación, se especifican los diferentes tipos de acceso remoto contemplados, junto a una lista de normas y recomendaciones para cada uno de ellos.

Con la financiación de la GENERALITAT VALENCIANA y FEDER
GENERALITAT VALENCIANA Conselleria de Sanitat Universal i Salut Pública
UNIÓN EUROPEA Fondo Europeo de Desarrollo Regional

4.1 Acceso individual por VPN

La utilización de una VPN o red privada virtual permite la creación de un túnel seguro mediante el cifrado de datos durante la conexión, otorgando acceso remoto seguro entre el equipo individual y la red de la empresa.

Para asegurar la autenticidad de extremo a extremo en un canal de comunicaciones, antes de intercambiar información deberá establecerse el uso de contraseñas acordes a la política de la organización.

Nota: Es muy recomendable el empleo de un doble factor de autenticación en todos los accesos remotos, con independencia de la categoría del sistema.

Se habilitará el registro de auditoría de las conexiones, incluyendo las direcciones IP origen y destino, fecha y hora de inicio y finalización de la conexión VPN, así como el ID de usuario que se conecta.

El algoritmo de cifrado empleado por la solución VPN será de los recomendados por el CCN en función de la categoría del sistema.

Para el empleo de accesos remotos basados en VPN, los usuarios deberán tener en cuenta:

- Es responsabilidad del usuario autorizado para acceder mediante VPN, asegurarse de que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso personal e intransferible para aquellos a quienes les ha sido asignada.
- La utilización de múltiples conexiones VPN desde un mismo equipo de usuario no está permitida, por lo que únicamente debe emplearse una conexión activa por usuario en un momento dado.
- La conexión VPN establecida será automáticamente desconectada si no se detecta actividad en un tiempo determinado de 60 minutos. El usuario deberá autenticarse nuevamente para reconectarse a la red.
- El equipo remoto desde el que se establecerá la conexión debe ser, por defecto, propiedad de la Organización, por lo que estará bastionado (configurado con criterios seguros) y con el antivirus actualizado.
- El acceso remoto a la red del Centro de Investigación Príncipe Felipe desde ordenadores públicos, entendiendo por estos aquellos que se alquilan por tiempo

de conexión, salas de internet de disponibilidad pública, cibercafés y similares, **está estrictamente prohibido**.

Si se requiere realizar la conexión remota VPN desde un equipo particular (BYOD), ésta requerirá autorización específica, debiendo adicionalmente tenerse en cuenta las siguientes consideraciones:

- El equipo deberá tener instalada y actualizada una solución antivirus, así como tener al día las actualizaciones de seguridad del sistema operativo y las aplicaciones.
- Queda prohibido dejar desatendido el equipo durante la jornada laboral, permaneciendo vigentes las normas generales del Centro de Investigación Príncipe Felipe orientadas al puesto de trabajo, como es bloquear el equipo cuando no esté atendido. Deberá liberarse la conexión VPN ante pausas que se prevean prolongadas.
- Mientras la VPN se encuentre conectada al Centro de Investigación Príncipe Felipe no deberán estar en ejecución aplicaciones personales.
- Si el equipo personal es empleado por más de un miembro de la familia, deberá existir un perfil de usuario independiente desde el que se realice la conexión VPN con el Centro de Investigación Príncipe Felipe.
- Además, teniendo en cuenta que en situaciones de teletrabajo se atienden llamadas y videoconferencias en abierto, habitualmente hablando a través del micrófono del equipo y escuchando a través de sus altavoces, se requerirá desactivar cualquier asistente virtual (tipo Alexa, Siri o similar) que pudiera estar en la habitación, donde nos encontremos, buscando con ello mantener la confidencialidad y secreto profesional.

4.2 Acceso por LAN to LAN

Se conoce como interconexión LAN to LAN al servicio de transmisión de datos punto a punto que permite conectar entre sí dos redes, por ejemplo, las correspondientes a dos sedes de una misma Organización, o la conexión de una sede con determinada red de un proveedor. Habitualmente dicho enlace entre redes, por cuestiones de seguridad, se realiza mediante una VPN a través de internet establecida entre dos dispositivos dedicados.

4.3 Acceso de Proveedores

Los proveedores que necesiten conectar de forma remota deberán enviar un correo electrónico al Área T.I. (informatica@cipf.es) con los datos de las personas que la usaran (nombre completo y NIF) y el motivo de la solicitud. El área de T.I. les enviará el documento DOC-007_Conformidad de VPN para que firmen la aceptación de las normas y usos. Una vez recibido el documento firmado, se procederá al alta y se remitirá a la entidad el documento DOC-008_Datos Usuario Acceso Remoto, que contiene las credencias.

Cuando la organización, ya sea por acuerdos o por servicios contratados, necesite brindar acceso a los proveedores con los que tenga alguna relación, deberá verificar de manera constante el acceso de terceros a los sistemas de la organización, llevando control de las cuentas o accesos compartidos:

- Segmentando la red física, limitando los accesos a los usuarios, cuentas y procesos informáticos únicamente a los recursos absolutamente necesarios para realizar las actividades rutinarias para las que se encuentran autorizados.
- Habilitando controles de permisos específicos: la utilización de soluciones de administración de accesos privilegiado para conceder únicamente los permisos necesarios y adecuados.
- Otorgando accesos remotos VPN al personal del proveedor que lo requiera, a ser posible con períodos finitos de vigencia, prorrogables.
- Revocando el acceso VPN al finalizar la relación contractual, o al ser sustituido el colaborador asignado por el proveedor.
- Realizando auditorías periódicas con el propósito de hallar y deshabilitar posibles accesos remotos que ya no sean necesarios.

4.4 Acceso a documentos compartidos y trabajo colaborativo

En la actualidad el Centro de Investigación Príncipe Felipe dispone de la solución NextCloud de compartición de documentos, así como de la plataforma colaborativa Office 365.

Se revisarán los permisos asignados a las carpetas y documentos que se almacenan en estas plataformas, asegurando que solo tienen permisos las personas adecuadas y los documentos no sean accesibles de forma pública.

Se establecerán las siguientes medidas de protección de los documentos:

- La documentación únicamente será accesible por las personas autorizadas, significa que los usuarios de la plataforma colaborativa o de compartición únicamente accederán a las carpetas o documentos autorizados, ya sea para consulta, descarga, modificación, supresión, así como para incorporar nuevos documentos.
- Se establecerán permisos a nivel de usuario o grupo de usuarios.
- Debe disponerse de trazabilidad respecto a los documentos.
- Es recomendable establecer mecanismos que permitan conocer si el documento se abre, o se intenta abrir, desde una ubicación desconocida o por un usuario sin permisos.

5. COMUNICACIÓN DE DEFICIENCIAS DEL PROCEDIMIENTO

Cualquier deficiencia y/o inconsistencia en este procedimiento deberá de ser puesta en conocimiento del Responsable de Seguridad (o la persona en la que delegue).

6. DOCUMENTACIÓN COMPLEMENTARIA

- Procedimiento de gestión de autorizaciones
- Normativa de Uso de Medios Electrónicos
- Formulario de Petición
- Guía CCN-STIC-836 Seguridad en Redes Privadas Virtuales (VPN)
- Guía CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad
- CCN-CERT BP/18 Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia.
- Checklist CCN-CERT BP-18 Seguridad para situaciones de teletrabajo.xls.

7. ANEXOS

7.1 Anexo- RECOMENDACIONES

El acceso remoto mediante VPN, así como las plataformas de compartición de documentos y colaboración, suponen riesgos, constituyendo, no obstante, una forma de conectividad esencial para el funcionamiento actual de las organizaciones. En aras de mitigar dichos riesgos, se establecen las siguientes mejores prácticas:

Gestión y control de hardware y sistemas operativos: Puede ser considerada la recomendación más básica, pero es importante tenerla en cuenta. Cuando se trata de otorgar acceso remoto a los colaboradores hay que tener en cuenta que accederán a la red desde diferentes dispositivos, los que pueden representar una amenaza en sí misma. Por ello, los dispositivos que se proporcionan al trabajador deben ser confiables, deben tener sistemas operativos y aplicaciones completamente actualizados y un antivirus de buena calidad. En cuanto a las sesiones de acceso e inicio de sesión en los dispositivos del trabajador es recomendable que tenga una cuenta personal y una cuenta diferente utilizada únicamente para el trabajo remoto.

Gestión de la seguridad física de los dispositivos: Pueden ocurrir ciertas situaciones como el robo del dispositivo de trabajo, ante las cuales deben tomarse medidas antes que sucedan, como por ejemplo medidas de protección antirrobo, de localización del dispositivo perdido o robado, cifrado del disco duro o de un repositorio del mismo o, incluso, un sistema de borrado remoto de datos.

Gestión de permisos de roles: Dentro de las organizaciones hay múltiples perfiles que, para garantizar la seguridad, no es necesario que todos ellos tengan acceso a la toda la información de la organización. Deben establecerse permisos dependiendo del puesto del trabajador o del tipo de trabajo que este realiza, de igual modo con las aplicaciones o programas que un trabajador de manera remota debe usar, estableciendo acceso restringido para lo que no sea necesario acceder en remoto. Por tal razón, deben gestionarse adecuadamente los permisos y accesos según el desempeño del empleado dentro de la organización.

Monitorización de la actividad de la red: Toda actividad dentro de la red debe ser monitorizada para identificar cualquier tipo de actividad sospechosa. Por tanto, debe considerarse si hay intentos fallidos repetidos de autenticación remota o de acceso remoto a recursos. Cualquier tipo de tráfico que parezca inapropiado debe ser controlado y monitorizado.

Gestión de Contraseñas y autenticación de dos factores: Las contraseñas son un factor determinante a la hora de mantener la seguridad en las organizaciones, puesto que permiten establecer criterios de acceso a los recursos. Razón por la que debe evaluarse

medidas que permitan mantenerlas seguras por ejemplo con el empleo de gestores de contraseñas. Otro aspecto importante debe tener la autenticación de doble factor para acceder a cualquier cuenta cuando se trabaja de manera remota.

Tomar en cuenta el factor humano: La identificación de riesgos como la explotación de vulnerabilidades deben extenderse al capital humano que opera en contacto con los dispositivos y sistemas asociados de acceso remoto a recursos de la organización. Por tanto, es de vital importancia concientizar y educar al personal para mitigar los riesgos informáticos a los que se expone la organización.

Con la financiación de la GENERALITAT VALENCIANA y FEDER
GENERALITAT VALENCIANA Conselleria de Sanitat Universal i Salut Pública
UNIÓN EUROPEA Fondo Europeo de Desarrollo Regional