ANEXO No. 9

ACUERDO DE NIVELES DE SERVICIOS DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES Y DE SEGURIDAD FISICA Y LOGICA

Proceso de Selección _____

Bogotá, D.C. _____

PROPONENTE: _____

ACUERDO DE NIVELES DE SERVICIOS DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

Servicio	ITEM	ANS	Definición	Medición	Nivel Requerido	Periodicidad	Aplica a
PROVISIÓN SERVICIOS DE INTERNET	1	Efectividad en la ampliación de ancho de banda.	Es la obtención del servicio de ampliación de ancho de banda	Número de horas requeridas para realizar la ampliación del ancho de banda.	24 horas	Conforme se defina en un Plan de Trabajo y Cronograma	Todas las solicitudes de ampliación del canal
	2	Disponibilidad Estándar	Posibilidad de transmisión de Información	Número de horas con disponibilidad para transmitir/Número de horas del respectivo periodo en el cual debe estar funcionando un aplicativo	99.60%	Conforme se defina en un Plan de Trabajo y Cronograma	Al canal
PROVISIÓN SERVICIOS DE INFRAESTRUTURA TIC	1	Tiempo en aprovisionamiento de infraestructura TIC	Capacidad de aprovisionar oportunamente infraestructura tecnológica	Tiempo Propuesto/ Tiempo Ejecutado	T Ejecutado <= T Propuesto	Por demanda para dar cumplimiento a las obligaciones del contrato	Infraestructura Tecnológica
GESTION DE CAMBIOS EN INFRAESTRUCTURA TIC	1	Ejecución de cambios requeridos	Cumplimiento del cronograma presentado para la ejecución de cambios	Diferencia entre el tiempo empleado para ejecutar la solicitud de cambio y el tiempo según cronograma	T<=8 días hábiles	Conforme se defina en un Plan de Trabajo y Cronograma	Todas las solicitudes de cambio
	2	MTTR (Mean Time To Restore)	Tiempo promedio de recuperación ante fallas.	Resolución de fallas en un tiempo promedio inferior al comprometido por disponibilidad	<= 4 horas severidad 1<= 8 horas severidad 2. Ver Nota al pie de la tabla)	Para dar cumplimiento a las obligaciones del contrato	Infraestructura Tecnológica
GESTIÓN DE SEGURIDAD	1	Aplicación de parches sobre la infraestructura de TI	Aplicación de parches de seguridad que minimicen la vulnerabilidad	Reporte de parches aplicados	Una vez el fabricante libera parches de actualización en un T<= 36 horas	De acuerdo a las vulnerabilidades detectadas en los productos software	Infraestructura Tecnológica
	2	Tiempos de atención y resolución de incidentes de seguridad	Tiempo requerido para solucionar un problema de seguridad	T respuesta= 4 hrs - T de atención y solución del incidente	T respuesta <= 4 horas Todas las incidencias de seguridad serán tratadas como severidad 1	Una vez se detecte o reporte el incidente	Infraestructura Tecnológica
	3	Sistema de Gestión de Calidad sobre los procesos TIC	Verificar que la entidad incluya sus procesos TIC en el Sistema de Gestión de Calidad	Verificar que en el SIG se incluya los procesos TIC de la entidad	100%	Al inicio del contrato	A las universidades y/ó IES

Nota: En cuanto a la tipificación de severidades se debe entender así: Severidad 1- Las aplicaciones se encuentran sin servicio y Severidad 2- Las aplicaciones se encuentran con servicio, pero éste es intermitente.

OPCION 1 “TRABAJO EN SITIO”

ACUERDO DE NIVELES DE SEGURIDAD FÍSICA Y LÓGICA

Sala de Verificación de Requisitos Mínimos, Sala de Valoración de Antecedentes, Sala de Construcción y/o Validación de Ítems y Ensamble de Pruebas Escritas de Competencias Laborales, Sala de Diseño de Cursos de Formación y Ensamble de la Evaluación Final de los Cursos de Formación, Sala de Ensamble de las Pruebas de Ejecución y Sala de Construcción y Ensamble de las Pruebas Especiales (Entrevista).

Para adelantar la verificación de requisitos mínimos (VRM), Valoración de Antecedentes (VA), Construcción y/o Validación de ítems, Ensamble de Pruebas Escritas, Diseño de Cursos y Ensamble de la Evaluación Final de los Cursos de Formación, Ensamble de las Pruebas de Ejecución y Sala de Construcción y Ensamble de las Pruebas Especiales (Entrevista), las salas deben estar dotadas mínimo con los siguientes sistemas y elementos:

Las salas físicas dispuestas por la IES se deben interconectar con las soluciones de la CNSC mediante una arquitectura tecnológica similar a la definida en el siguiente diagrama:

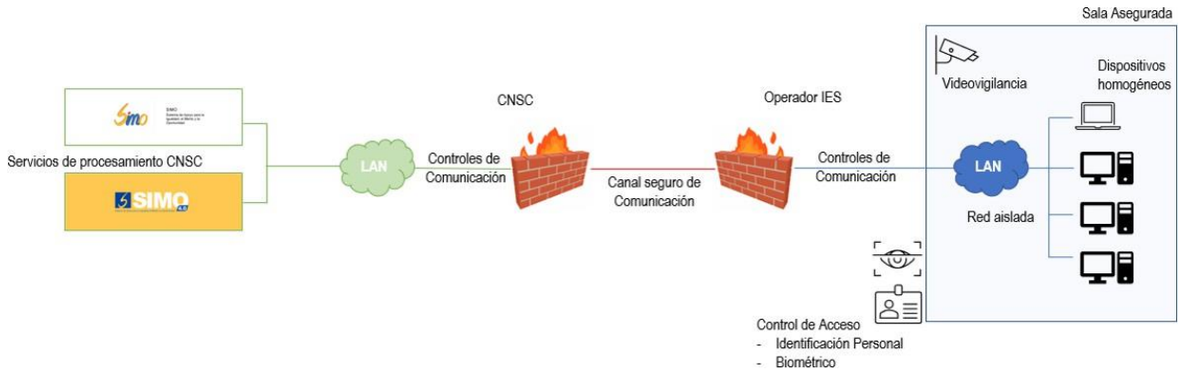


Ilustración 1. Esquema genérico de conexión de salas de trabajo aseguradas que acceden a los servicios de la CNSC

Ítem	Requerimiento
1	Sistema de Circuito Cerrado de Televisión (CCTV) que permita capturar toda la actividad que se presente en dicha sala y que registre el ingreso y salida del personal.
2	Sistema de control de acceso electrónico; ya sea control táctil, tarjetas de proximidad o terminal de reconocimiento facial, que almacene el registro de ingreso y salida.
3	Durante esta etapa los equipos de cómputo asignados sólo deben ser de uso exclusivo del proceso de selección contratado.
4	Se debe garantizar que NO se pueda realizar copia de información de los equipos a través de medios extraíbles o removibles ni a través de la red o cualquier otro medio.
5	Los equipos de cómputo deben estar aislados, a través de una red LAN cableada (velocidad 100/1000 Mbps) independiente de las demás redes implementadas. Cableado estructurado debidamente certificado el cual debe incluir como mínimo red de datos Cat 6 o superior y corriente regulada con un sistema ininterrumpido de potencia UPS con capacidad suficiente de suplencia de energía para evitar la pérdida de datos.
6	Aprovisionar dos enlaces de conectividad IP con un ancho de banda simétrico garantizando un nivel de reuso 1:1 dedicado para el servicio de internet con un ancho de banda mínimo de 20 Mbps, con capacidad de ser ampliados por demanda en caso de que esto se requiera, mediante enlace físico de fibra óptica en su conexión de última milla. Dichos canales deben ser de uso exclusivo para los procesos de selección que se encuentre adelantando y es de uso exclusivo para las salas asignadas para la ejecución de cada una de las etapas del proyecto con sus respectivas fases de reclamaciones. Lo anterior para garantizar HA en caso de falla de uno de los canales.

7	Desde los equipos de cómputo sólo se debe poder ingresar a la(s) aplicaciones dispuestas para tal fin; el acceso a internet debe estar totalmente restringido, sólo se permitirá el acceso a las URL estrictamente necesarias para adelantar el proceso. Nota: la Sala de Construcción de Ítems (conjunto de preguntas, respuestas y distractores de respuesta), Diseño de Pruebas, Sala de Diseño de Cursos de Formación, Sala de Construcción y/o Validación de Ítems y Ensamble de Pruebas Escritas y de la Evaluación Final de los Cursos de Formación, Sala de Ensamble de las Pruebas de Ejecución y Sala de Construcción y Ensamble de las Pruebas Especiales (Entrevista), podrá tener acceso únicamente a los recursos tecnológicos internos (LAN) necesarios (aplicaciones, URL, etc.) dispuestos por la Universidad y/o lES. Las salas de trabajo para Verificación de Requisitos Mínimos, Valoración de Antecedentes, para Construcción y/o Validación de Ítems y Ensamble de Pruebas Escritas de Competencias Laborales, para Diseño de Cursos de Formación y Ensamble de la Evaluación Final de los Cursos de Formación, para el Ensamble de las Pruebas de Ejecución y Sala de Construcción y Ensamble de las Pruebas Especiales (Entrevista), que accedan a los recursos de procesamiento de información prestados por la CNSC, deben tener acceso autorizado por los canales de comunicaciones que se han establecido, según el numeral 6 de esta sección.
8	La sala destinada para la Construcción y/o Validación de ítems (conjunto de casos, enunciados, respuestas y distractores de respuesta), la Sala de Ensamble de las Pruebas de Ejecución (tareas), y para las Pruebas Especiales (Entrevista - construcción de casos, preguntas y formatos de evaluación), no tendrá acceso a internet y debe estar totalmente aislada de las demás redes; el material digital de consulta deberá ser centralizado en un solo equipo haciendo uso de un medio de almacenamiento externo que se debe habilitar solamente para este propósito y se debe deshabilitar una vez sea cargada la información o material de referencia. Desde este computador se compartirá de manera controlada a los demás. Nota: Este punto solo aplica para los procesos que incluyan construcción y/o validación de ítems (conjunto de preguntas, respuestas y distractores de respuesta), así mismo, para la prueba de ejecución que comprende la evaluación de competencias específicas del aspirante mediante la observación de la ejecución que debe hacer de una serie de tareas propias del empleo y para la prueba especial (entrevista) se relaciona a la construcción de casos, preguntas y formatos de evaluación. El operador que haga uso de software especializado para la construcción ítems que se presta a través de servicios en nube (FastTest – Synap - Exambuilder), debe realizar el control (aplicar restricciones) de internet basado en listas blancas.
9	El ingreso y salida de cualquier material y/o elemento de las salas asignadas para la ejecución de cada una de las etapas del proyecto como son Verificación de Requisitos Mínimos (VRM), Valoración de Antecedentes (VA), Construcción y/o Validación de ítems y Ensamble de Pruebas Escritas, Diseño de Cursos y Ensamble de la Evaluación Final de los Cursos de Formación, Ensamble de las Pruebas de Ejecución y Construcción y Ensamble de las Pruebas Especiales (Entrevista) debe ser controlado, documentado y aprobado sólo por el responsable de esta etapa del proceso de selección.
10	Se debe contar con un inventario detallado de los equipos de cómputo de características homogéneas, cuya configuración esté acorde con las configuraciones de procesamiento, almacenamiento, memoria y sistema operativo disponibles para el último semestre en el mercado tecnológico, como por ejemplo Microsoft Windows 10 Pro o última versión o alguna distribución de Linux con soporte, en versiones estables liberadas por los fabricantes. En caso de requerir incluir al inventario un nuevo equipo, se deberá notificar a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC de la CNSC quien autorizará el ingreso del equipo y podrá validarlo en cualquier momento durante la ejecución de la etapa. En los casos en donde se autorice una política de BYOD, el colaborador del proceso que aporta su dispositivo personal debe: a. Aceptar la instalación de las herramientas necesarias para el control dispuestos por la IES. b. Comprometerse a no usar repositorios locales (disco duro fijo, memorias o discos extraíbles) para la construcción de documentos intermedios de gestión o para realizar localmente la validación de los archivos vinculados por los aspirantes que están relacionados con el proceso de selección. c. Conceder derechos de revisión del contenido de los repositorios de almacenamiento de información locales, por parte de los supervisores del contrato o por cualquier proceso de auditoría que adelante la CNSC para validar el avance de las actividades del cronograma propuesto por la IES para esta etapa. d. Acogerse a las medidas de control, monitoreo y revisión que la IES adopte para los dispositivos aportados al proceso como si fuese parte del inventario de equipos administrados por la IES. Permitir el acceso remoto para realizar actividades de borrado seguro de los contenidos, archivos o datos que la mesa de ayuda de la IES identifique como información relacionada

	con el proceso de selección con el cual está vinculado.
11	Los equipos asignados a los usuarios deben pasar por al menos por una auditoria de la IES, donde se garantice el óptimo funcionamiento del equipo y el cumplimiento de estos requerimientos expuestos en este anexo para cualquiera de las salas propuestas. En el caso en donde la IES obtenga una autorización explicita de la CNSC para aplicar una política de BYOD, es necesario aclarar a los usuarios que estos equipos solamente pueden ser retirados de las salas de seguridad hasta que terminen las etapas correspondientes y se hayan aplicado todas las condiciones de revisión y borrado a las cuales se adhieren por acceder a esta modalidad de trabajo.
12	Los videos de las Cámaras de Vigilancia se deben conservar como parte de evidencia ante un posible reclamo y/o solicitud y con el fin de poder establecer si el protocolo de seguridad se cumplió a cabalidad. Esta información quedará disponible hasta por 5 años a disposición de la CNSC.
13	El acceso a las aplicaciones autorizadas debe ser exclusivamente desde los equipos designados al proyecto; por ningún motivo se debe tener acceso a estas aplicaciones desde las demás redes implementadas, excepto cuando la CNSC lo requiera.
14	La entrega de información por parte de las universidades o IES a la CNSC debe cumplir con el protocolo de seguridad establecido por la CNSC.
15	Una vez finalizadas estas etapas, se debe realizar un borrado seguro de la información contenida en los equipos, actividad que será verificada por la DTIC de la CNSC.

NOTA 1: Todo el personal involucrado en estos procesos debe firmar el Acuerdo de Confidencialidad en el manejo de la información a la cual tienen acceso y debe ser capacitado en el plan de seguridad del proceso, con respecto a sus directrices, aplicación y accionar en caso de que se presente un fallo en la seguridad de la información.

NOTA 2: En las salas no se debe poder ingresar: dispositivos de almacenamiento de datos o memoria externa, celulares, cámaras, ni ningún dispositivo o elemento que permita extraer información, de acuerdo con los criterios del Protocolo de Seguridad implementado para el proceso.

Según lo previsto en el artículo 31 numeral 3 de la Ley 909 de 2004, “Las pruebas aplicadas o a utilizarse en los procesos de selección tienen carácter reservado, sólo serán de conocimiento de las personas que indique la Comisión Nacional del Servicio Civil en desarrollo de los procesos de reclamación”.

NOTA 3: El uso de la sala de Construcción y/o Validación de ítems (conjunto de preguntas, respuestas y distractores de respuesta) será facultativo por parte del constructor, así como la construcción de casos, preguntas y formatos de evaluación para la prueba especial (entrevista). Sin embargo, para el diseño y ensamble de las pruebas sí será obligatorio su uso.

NOTA 4: El uso de las salas será de uso exclusivo para atender las etapas del Proceso de Selección durante el periodo que duren las mismas.

NOTA 5: Las salas indicadas en el capítulo “***Sala para el Diseño de Cursos de Formación y Ensamble de la Evaluación Final de los Cursos de Formación***” (tablas numeradas como 4. Diseño y Evaluación Final de los Cursos de Formación), son de uso exclusivo para atender de forma específica las actividades de diseño y evaluación final de los cursos de formación durante el periodo que duren las mismas, para los procesos de selección que la requieran.

NOTA 6: La Sala de Ensamble de las Pruebas de Ejecución y de Ensamble y Construcción Pruebas Especiales (Entrevista), son de uso exclusivo para atender de forma específica las actividades que requieran revisión, construcción, diagramación, ensamble, impresión, calificación de las pruebas, durante el periodo que duren las mismas, para los procesos de selección que lo requieran.

OPCIÓN 2 "TRABAJO REMOTO"

ACUERDO DE NIVELES DE SEGURIDAD FISICA Y LOGICA

Verificación del cumplimiento de Requisitos Mínimos, Valoración de Antecedentes, Sala de Construcción y/o Validación de Ítems, Ensamble de Pruebas Escritas, Sala de Diseño y Ensamble de la Evaluación Final de los Cursos de Formación, Sala de Ensamble de las Pruebas de Ejecución y Sala de Construcción y Ensamble de las Pruebas Especiales (Entrevista).

Para la ejecución de las etapas Verificación de Requisitos Mínimos (VRM), Valoración de Antecedentes (VA), bajo la opción de trabajo remoto, la IES debe implementar una arquitectura tecnológica similar a la definida en el siguiente diagrama:

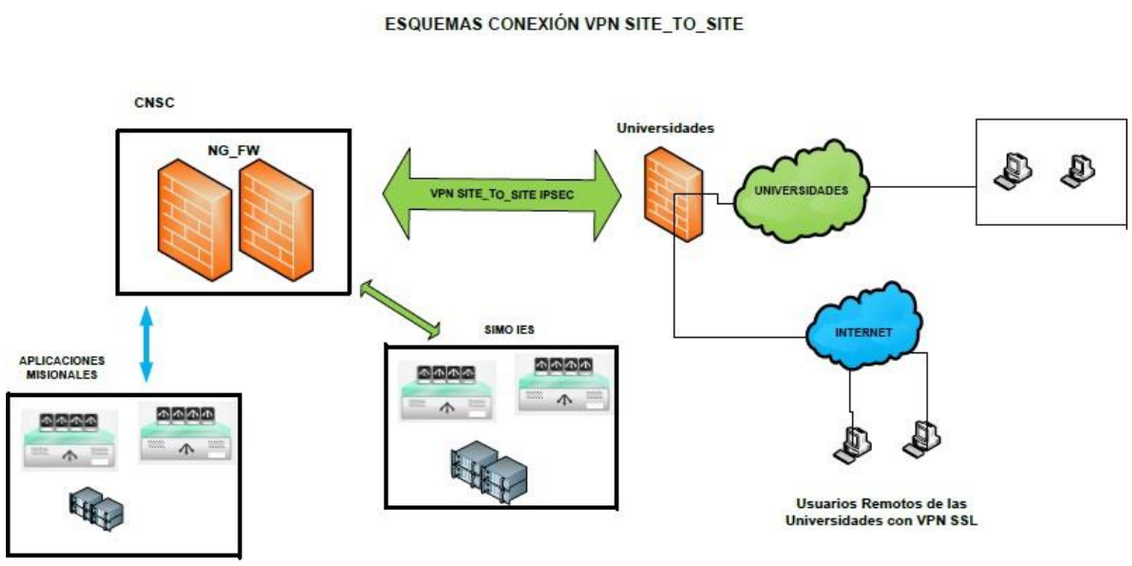


Ilustración 2. Esquema de conexión segura entre sitios, con acceso remoto controlado

Para adelantar las etapas descritas anteriormente, la IES debe cumplir con los siguientes aspectos del sitio central que la IES defina al que se conectarán sus usuarios o colaboradores:

1. Características Sitio Central	
DENOMINACIÓN TÉCNICA:	**Especificaciones técnicas sitio central**
ÍTEM	**CARACTERÍSTICA**
1.1	Los equipos de comunicaciones de borde que permiten la conectividad de los dispositivos de cómputo deben soporta la creación de redes locales virtuales (Vlan), listas de acceso y una capacidad mínima de rendimiento superior a (Throughput up to) 90 Mbps, capacidad de conmutación (Switching capacity) de 100 Gbps. Para los equipos de centrales (equipos core) que conectan a los equipos de borde, deben soportar una capacidad mínima de Throughput de 300 Mbps. Los equipos de perimetral seguridad que reciben la conexión a internet deben soportar como mínimo una capacidad de 50 Gbps de Throughput, IPsec VPN Throughput 40 Gbps, SSL-VPN Throughput 3Gbps. Los servidores que estén en la ubicación que defina la IES como punto centralizado donde se conecten sus usuarios deben estar aislados, a través de una red LAN cableada (velocidad 100/1000 Mbps) independiente de las demás redes implementadas. Cableado estructurado debidamente certificado el cual debe incluir como mínimo red de datos Cat 6 o superior y corriente regulada con un sistema ininterrumpido de potencia UPS con capacidad suficiente de suplencia de energía para evitar la pérdida de datos.

1. Características Sitio Central	
DENOMINACIÓN TÉCNICA:	**Especificaciones técnicas sitio central**
ÍTEM	**CARACTERÍSTICA**
1.2	Aprovisionar dos enlaces dedicados a Internet en IPv4 e IPV6 con un ancho de banda simétrico garantizando un nivel de reuso 1:1 dedicado para el servicio de internet con un ancho de banda mínimo de 20 Mbps, con capacidad de ser ampliados por demanda en caso de que esto se requiera, mediante enlace físico de fibra óptica en su conexión de última milla. Dichos canales deben ser de uso exclusivo para los procesos de lo(s) Procesos de Selección que se encuentre(n) adelantando y es de uso exclusivo para las salas asignadas para la ejecución de cada una de las etapas del proyecto con sus respectivas fases de reclamaciones. Lo anterior para garantizar alta disponibilidad (HA) en caso de falla de uno de los canales.
1.3	La sala destinada para la realización de las etapas de VRM / VA no tendrá acceso a internet y debe estar totalmente aislada de las demás redes, el material digital de consulta deberá ser centralizado en un solo equipo haciendo uso de un medio de almacenamiento externo que se debe habilitar solamente para este propósito y se debe deshabilitar una vez sea cargada la información o material de referencia. Desde este computador se compartirá de manera controlada a los demás.
1.4	Se podrán implementar soluciones basada en equipos de cómputo de características homogéneas y cuya configuración esté acorde con las configuraciones de procesamiento, almacenamiento, memoria y sistema operativo disponibles para el último semestre en el mercado tecnológico, como por ejemplo Windows 10 Pro o última versión estable liberada por el fabricante o distribuciones de Linux son suscripción de soporte. En caso de requerir incluir al inventario un nuevo equipo, se debe informar a la DTIC – CNSC quien autorizará el ingreso del equipo y será validado en cualquier momento durante la ejecución de la etapa. También se podrán implementar soluciones basadas en escritorios virtuales o estaciones remotas en cuyo caso las máquinas virtuales deben mantener las especificaciones o su equivalente de los equipos físicos anteriormente descritos. Para los casos en donde se autorice una política de BYOD el colaborador del proceso, que aporta su dispositivo personal debe: a. Aceptar la instalación de las herramientas necesarias para el control y soporte remoto dispuestos por la IES. b. Comprometerse a no usar repositorios locales (disco duro fijo, memorias o discos extraíbles) para la construcción de documentos intermedios de gestión o para realizar localmente la validación de los archivos vinculados por los aspirantes que están relacionados con el proceso de selección. c. Conceder derechos de revisión del contenido de los repositorios de almacenamiento de información locales, por parte de los supervisores del contrato o por cualquier proceso de auditoría que adelante la CNSC para validar el avance de las actividades del cronograma propuesto por la IES para esta etapa. d. Acogerse a las medidas de control, monitoreo y revisión que la IES adopte para los dispositivos aportados al proceso como si fuese parte del inventario de equipos administrados por la IES. e. Permitir el acceso remoto para realizar actividades de borrado seguro de los contenidos, archivos o datos que la mesa de ayuda de la IES identifique como información relacionada con el proceso de selección con el cual está vinculado.
1.5	El acceso a las aplicaciones autorizadas debe ser exclusivamente desde los equipos designados al proyecto. Por ningún motivo se debe tener acceso a estas aplicaciones desde las demás redes implementadas, excepto cuando la CNSC lo requiera.
1.6	La entrega de información por parte de las universidades o IES a la CNSC debe cumplir con el protocolo de seguridad establecido por la Entidad.
1.7	Una vez finalizadas estas etapas, se debe realizar un borrado seguro de la información contenida en los equipos, actividad que será verificada por la DTIC de la CNSC.
1.8	Para los casos en donde se haya autorizado explícitamente el uso de una política de BYOD, se deben definir y posteriormente poder evidenciar las condiciones de uso de los equipos de los usuarios finales, los controles tecnológicos aplicables y la suscripción de una aceptación de acogimiento de las políticas y controles de seguridad dispuestos por la IES de parte del propietario del dispositivo, como sí el equipo aportado hiciera parte del inventario de la IES hasta la culminación de la etapa correspondiente.

CONDICIONES TECNOLÓGICAS DE OPERACIÓN PARA TRABAJO REMOTO PARA LAS ETAPAS DE VERIFICACIÓN DE REQUISITOS MÍNIMOS Y VALORACIÓN DE ANTECEDENTES

Para el trabajo remoto o trabajo en casa para los colaboradores de la Institución de Educación Superior – IES, se deberán desarrollar las siguientes condiciones de seguridad:

2. Verificación cumplimiento de Requisitos Mínimos y Valoración de Antecedentes,		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para Verificación cumplimiento de Requisitos Mínimos y Valoración de Antecedentes**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
2.1	Personal	• Contar con los registros actualizados y firmados de los acuerdos de confidencialidad y no divulgación suscritos entre la IES y los colaboradores que van a intervenir en alguna actividad de la ejecución de las pruebas que se han suscrito contractualmente entre la IES y la CNSC. • Se debe identificar y mantener actualizada la relación de personal autorizado para acceder de manera remota segura a estos servicios. • Se debe contar con registros de capacitación (que incluya entrenamiento y concienciación) de la IES a sus colaboradores sobre las condiciones de confidencialidad, protección y no divulgación de la información que se hacen extensivas a las conexiones remotas autorizadas. • Se debe contar con registros de capacitación de la IES a sus colaboradores sobre la importancia de mantener actualizados y debidamente protegidos los equipos de acceso remoto del personal autorizado, en caso de utilizar la modalidad de BYOD (Bring Your On Device) para permitir este tipo de operación remota. • Se debe contar con registros de capacitación de la IES a sus colaboradores sobre la importancia de la adopción de contraseñas (password) fuertes y protección de las credenciales de acceso (usuario y contraseña), como recursos únicos, personales e intransferibles de autenticación ante las diversas plataformas de procesamiento de información relacionadas con el desarrollo de las etapas del proceso de selección que se han suscrito contractualmente entre la IES y la CNSC. • Mantener canales de comunicación permanente entre el personal autorizado y la supervisión de operación tecnológica (Mesa de servicio) por parte de la IES, para identificar de manera proactiva posibles fallas o ataques informáticos que se pudiesen presentar por hacer uso de redes públicas.

2. Verificación cumplimiento de Requisitos Mínimos y Valoración de Antecedentes		
DENOMINACIÓN TÉCNICA		**Conexión remota a la IES para Verificación cumplimiento de Requisitos Mínimos y Valoración de Antecedentes**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
2.2	Aspectos Técnicos	• Se deben adecuar los equipos de cómputo de cada uno de los analistas con la versión actualizada de un software antivirus, un software antimalware y la última versión del programa de acceso remoto a implementar, para lo cual se debe indicar el software de acceso remoto y antivirus instalado y sus versiones. • El acceso remoto debe contar con tres (3) métodos de autenticación con usuario y clave robusta. La primera clave será la que pide el software de conexión remota; la segunda clave le debe permitir al analista ingresar al sistema operativo del equipo que sea asignado por la IES; y la tercera clave será la que debe introducir para poder ingresar al SIMO. • No se debe permitir el acceso remoto desde computadores distintos a los definidos por los analistas como su estación de trabajo del hogar. • Se debe realizar una verificación periódica y remota de cada equipo de los analistas para garantizar el correcto funcionamiento de la máquina junto con test de velocidad de acceso a internet y posibles recomendaciones, lo cual se hará cada quince (15) días y se dejará registro de esta actividad por equipo. • La IES debe adecuar de manera remota la configuración de los equipos del hogar de los analistas para una correcta y estable conexión con las estaciones de trabajo que tienen asignadas por las IES. Estas actividades deben quedar relacionadas en una bitácora que permita ver en qué fecha se verificó y a que PC de usuario se le hizo la revisión. • La IES solo permitirá el acceso remoto a las estaciones de trabajo física o virtual adecuadas en las instalaciones definidas por las IES mediante el software especializado informado y avalado por la CNSC, lo cual se hará mediante una herramienta tecnológica que se encargará de gestionar todos los protocolos de seguridad y permisos solo a los equipos registrados de los integrantes del equipo de Verificación de Requisitos Mínimos y de Valoración de Antecedentes. Para lo anterior el operador debe informar a la CNSC qué herramienta tecnológica utilizará con su marca y versión correspondiente.

2.3	Aspectos de Telecomunicaciones y Seguridad	• La IES debe propender porque se mantenga operativo los canales o medios de comunicación establecido entre la IES y la CNSC. Para lo cual mensualmente se enviará un reporte de operación del canal de datos donde se pueda verificar el estado de operación. • Habilitar los canales de telecomunicación apropiados para permitir que los colaboradores autorizados por la IES puedan acceder de manera remota segura a los servicios de la IES y desde allí lograr el acceso a la CNSC. • Gestionar de manera adecuada el ancho de banda que ingresa desde las conexiones remotas de los usuarios autorizados hacia las instalaciones de la IES. • Validar el adecuado enrutamiento de acceso remoto seguro del personal autorizado hacia los servicios autorizados por la CNSC para la gestión de las obligaciones suscritas. Lo cual se verificará mediante pruebas de traceroute desde el diez por ciento (10%) de los equipos avalados, las cuales debe enviarse a la CNSC desde el inicio del trabajo remoto. • Monitorear el uso de los canales de acceso remoto hacia la IES, entregando o reasignando los parámetros de prioridad que sean establecidos para los diferentes perfiles de usuario que puedan acceder a los servicios de la CNSC. • Usar medios de comunicación segura a través de túneles asegurados mediante protección de acceso no autorizado y métodos de cifrado asimétricos entre los PC del personal autorizado para el trabajo remoto y la sede de la IES que enrute las comunicaciones hacia la CNSC mediante la implementación de VPN, para lo cual la IES deberá indicar que herramienta tecnológica gestiona estos túneles. • La IES no debe hacer uso de utilitarios de punto a punto (P2P - pear to pear) o de acceso directo a equipos para otorgar el acceso del personal asignado para la ejecución de las pruebas que forman parte del contrato suscrito con la CNSC. • El establecimiento de los túneles seguros de comunicaciones debe contar al menos con mecanismos de autenticación fuerte (usuario y contraseña robusta), que incluyan múltiples factores de autenticación y cifrado de la información que se trance. • Se debe garantizar que todos los elementos de telecomunicaciones sean desplegados por la IES para adoptar el acceso remoto seguro y se encuentran debidamente actualizados a las últimas versiones estables disponibles. Para lo cual se hará una revisión acompañada por la DTIC donde se verifique aleatoriamente las versiones de actualización de sus equipos de telecomunicaciones. • Se deben mantener y revisar constantemente los registros automáticos de eventos (gestión de logs), de las conexiones remotas establecidas. Estos logs deben estar disponibles en algún medio donde la CNSC pueda consultarlos en compañía de la IES. • Se debe garantizar que las herramientas de control de acceso remoto seguro estén configuradas de tal forma que se impida el acceso a las unidades de almacenamiento local del cliente de conexión, evitar la transferencia de archivos, hacer captura de pantalla (print screen) y limitar el acceso en la sesión del usuario a correos gratuitos tipo Gmail, Hotmail, entre otras plataformas gratuitas. • La red de la IES debe estar protegida perimetralmente por dispositivos de seguridad tipo firewalls. En aquellos casos en donde el contrato suscrito y vigente, no haya exigido el uso de dispositivos de seguridad perimetral con funcionalidades de firewall de última generación, la IES deberá propender por contar con servicios locales de cortafuegos de los equipos de usuario final tanto en los computadores ubicados en las salas autorizadas, como en los equipos de cómputo remotos de los usuarios autorizados. • Se deben desplegar herramientas de monitoreo y control de la velocidad de internet para los canales virtuales o túneles asegurados establecidos entre la IES y los sitios de acceso remoto autorizados de sus colaboradores, con el propósito de mantener los niveles de operación necesarios para cumplir con los compromisos suscritos entre la IES y la CNSC.

CONDICIONES TECNOLÓGICAS DE OPERACIÓN DE TRABAJO REMOTO PARA LA CONSTRUCCION Y VALIDACIÓN DE ÍTEMS Y PARA LA CONSTRUCCIÓN DE CASOS Y PREGUNTAS Y DE FORMATOS DE EVALUACIÓN (PRUEBA DE ENTREVISTA)

Para la ejecución de Construcción y Validación de ítems, la construcción de casos y preguntas y formatos de evaluación, bajo la opción de trabajo remoto la IES debe implementar una arquitectura tecnológica similar a la definida en el siguiente diagrama:

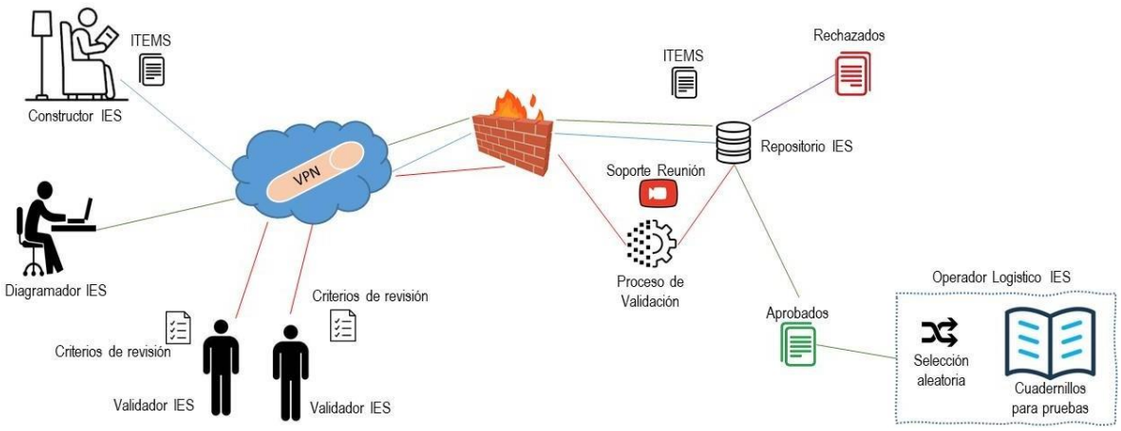


Ilustración 3. Esquema de conexión remota para la construcción y validación de ítems.

La implementación de la solución debe cumplir con las siguientes condiciones y características tecnológicas:

3. Construcción y validación de ítems y ensamble de pruebas escritas, construcción de casos y preguntas, formatos de evaluación y ensamble de pruebas especiales (Entrevista).		
3.1 Comunicaciones		
DENOMINACIÓN TÉCNICA		**Conexión remota a la IES para Construcción y Validación de Ítems y Ensamble de Pruebas Escritas, Construcción de casos y preguntas, formatos de evaluación y ensamble de las pruebas especiales (entrevista).**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**

3.1.1	Conexión remota	• Se debe garantizar que cada uno de los colaboradores de la IES cuente con un acceso remoto seguro y auditable a la infraestructura de la Institución de Educación Superior – IES. El nivel de auditoría por lo menos debe permitir observar: usuario conectado, fecha, hora de conexión y desconexión.
		
		• Siempre que se realice una conexión de escritorio remoto al equipo del colaborador esta deberá anunciársele con el fin de tener que esta no sea invasiva y altere su estado de privacidad.
		
		• El colaborador durante el desarrollo de su trabajo debe abstenerse de realizar actividades de carácter personal en el dispositivo de trabajo remoto destinado para el trabajo.
		Nota: el uso de smartphones está prohibido como terminal de trabajo remoto.
		
		• Si es posible habilitar una conexión con un segundo factor de autenticación la IES debe mantenerse este esquema durante la ejecución del contrato.
		
		• Configuración de registros automáticos revisables de:
		  • Administración de cuentas
		  • Inicios y cierre de sesión
		  • Acceso DC
		  • Acceso a objetos
		  • Uso de privilegios
		  • Sistema

3. Construcción y Validación de ítems y Ensamble de Pruebas Escritas, construcción de casos y preguntas, formatos de evaluación y ensamble de pruebas especiales (Entrevista).		
3.1 Comunicaciones		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para Construcción y Validación de Ítems y Ensamble de Pruebas Escritas- Construcción de casos y preguntas, formatos de evaluación y ensamble de las pruebas especiales (entrevista).**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**

3.1.2	Seguridad Remota	• Cada acceso remoto debe configurarse de manera que el colaborador no pueda conectarse a ninguna otra red mientras esté utilizando la conexión remota de la IES. Cada computador de los colaboradores debe ser inspeccionado remotamente por el personal técnico de la IES utilizando una herramienta tipo software de soporte remoto.
		• De forma automática, el sistema de autenticación deberá validar el cumplimiento de las características mínimas de seguridad de equipos o dispositivos de los colaboradores descritas en este numeral, para que permita la conexión remota.
		• El colaborador debe extremar las precauciones para evitar el acceso no autorizado a la información personal, propia y de terceros, manejada, no dejando a la vista ningún soporte de información en el lugar donde se desarrolle el trabajo remoto y bloqueando las sesiones de los dispositivos cuando estos estén desatendidos.
		• Cualquier anomalía que pueda afectar a la seguridad de la información debe notificarse al responsable del área de tecnología de la IES, a la mayor brevedad posible, a través de los canales definidos para el efecto.
		• Se debe contar con una configuración detallada de las de reglas de entrada y salida del cortafuegos (lógico o físico) de la IES.
		  • Acciones: permitir o bloquear
		  • Protocolos IP
		  • Direcciones IP entrada / salida

3.1.3	Equipos o dispositivos de los colaboradores	• El colaborador debe contar con una conexión a internet en su lugar de residencia, con un operador reconocido en el mercado colombiano, avalado por el ministerio de las tecnologías de la información y las comunicaciones (MINTIC). • La IES debe validar que la conectividad del equipo se realice mediante una conexión segura de internet, en lo posible usar conectividad cableada y que el equipo o dispositivo del colaborador tenga la red inalámbrica deshabilitada. • Se recomienda que la velocidad mínima contratada por el colaborador con el operador o ISP sea de 20 Mbps. Si se cuenta con Cámara IP externa, esta debe ubicarse de manera tal que cubra el espacio de trabajo. En caso de ser una cámara interna, debe cerciorarse que funciona adecuadamente y no tener elementos que la cubran.

3. Construcción y Validación de ítems y Ensamble de Pruebas Escritas, construcción de casos y preguntas, formatos de evaluación y ensamble de pruebas especiales (Entrevista).		
3.1 Comunicaciones		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para Construcción y Validación de Ítems y Ensamble de Pruebas Escritas- Construcción de casos y preguntas, formatos de evaluación y ensamble de las pruebas especiales (entrevista).**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
3.1.4	Registros automáticos de control (Logs) y auditoría	• Se debe llevar un registro detallado de hora, fecha, dirección IP origen y usuario que se ha conectado al acceso remoto. • Se debe llevar una bitácora de revisión de cumplimiento de los requisitos mínimos de los equipos de los colaboradores. • La IES debe programar revisiones aleatorias diarias, para validar el cumplimiento de las condiciones mínimas de operación de los equipos o dispositivos de los colaboradores. La CNSC puede realizar auditoría en cualquier momento para verificar el cumplimiento de las condiciones, para lo cual el ingeniero designado por la CNSC contactará al ingeniero asignado por la IES y de esta manera coordinar la actividad. • Se debe llevar registro tipo checklist, por el personal técnico de la IES, donde detalle fecha y hora, nombre del colaborador revisado, nombre de la persona técnica que revisa el equipo, este registro debe ser digital y estar disponible en un repositorio para su consulta por parte de la CNSC.
3.1.5	Soporte	• La IES debe contar con una mesa de servicio, donde se registren los requerimientos de los colaboradores, generando un identificador único por cada requerimiento, registrar cada seguimiento y evidencias gráficas de los servicios de apoyo a los colaboradores y a sus dispositivos de trabajo. • La IES debe contar con una herramienta de apoyo remoto de parte de la mesa de servicios que permita registrar el tipo de soporte dado, fecha y hora, de todos los servicios de apoyo que realiza esta mesa de servicio a los colaboradores.
3.1.6	Gestión de los Equipos de Conectividad	• La gestión de los equipos de comunicaciones debe realizarse mediante un protocolo de comunicaciones seguro y desde una Vlan en particular (Vlan de Gestión).
3.1.7	Interfaces de Conectividad	• Se requiere que el equipo de conectividad (Switch) cuente con interfaces de 1Gpbs/10Gbps, en lo posible Interfaces de 10 Gbps para la conexión con los equipos de seguridad perimetral – Firewall que debe soportar como mínimo una capacidad de 50 Gbps de Throughput, IPsec VPN Throughput 40 Gbps, SSL-VPN Throughput 3Gbps.

3. Construcción y Validación de ítems y Ensamble de Pruebas Escritas, construcción de casos y, preguntas, formatos de evaluación y ensamble de pruebas especiales (Entrevista).		
3.2 Seguridad		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para Construcción y Validación de Ítems y Ensamble de Pruebas Escritas - Construcción de casos y preguntas, formatos de evaluación y ensamble de las pruebas especiales (entrevista) – Condiciones de Seguridad.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
3.2.1	Equipos o dispositivos de los colaboradores	• Debe contar con un sistema operativo soportado por el fabricante a la fecha de inicio de labores y compatible con la infraestructura software que implemente la IES. • El sistema operativo, en el caso de requerir licenciamiento, debe ser licencia original emitida por el fabricante del hardware o del sistema operativo. • Para permitir conexión remota, se debe verificar y registrar por parte de la IES, en cada equipo o dispositivo del colaborador, las versiones de parches, hotfix o actualizaciones aplicadas correctamente a las últimas versiones liberadas por el fabricante. • El equipo o dispositivo del colaborador, debe contar con un sistema de antivirus reconocido, totalmente licenciado, se debe verificar y registrar por parte de la IES, las versiones de parches, hotfix o actualizaciones aplicadas correctamente a las últimas versiones liberadas por el fabricante. • El equipo o dispositivo del colaborador debe contar con un software de firewall, instalado y activo, se debe verificar y registrar por parte de la IES la funcionalidad del software de firewall. • Se debe generar una política de seguridad en el equipo del colaborador que, en el momento de establecer una conexión remota, se deshabiliten los puertos USB, unidades de CD, DVD, no se permita la redirección de dispositivos locales, ni a los equipos remotos en la IES. • Se debe permitir el establecimiento de una conexión de auditoría con el colaborador, donde se permita grabar y ver el entorno del colaborador, ya sea a través de la cámara web del equipo u otro mecanismo de grabación.
3.2.2	Locación física del colaborador	• La IES debe velar, auditar y registrar, para que las condiciones, tanto físicas como ambientales, donde labora el colaborador, sea en un lugar aislado, cerrado, sin distractores, ni acompañantes y que, en caso de ser necesario, registrar por medio de video dicho entorno. • Se debe crear, aplicar y sensibilizar a los colaboradores sobre la política de NO uso de celular, tablets, relojes inteligentes o televisores, mientras se realizan las actividades propias del objeto contractual, y en lo posible, la universidad debe registrar y guardar dichas evidencias. • La ejecución de las actividades de esta etapa tiene como propósito principal la producción de información sensible para el proceso de selección, que cuentan con reserva de acceso a ella, razón por la cual se debe indicar a los colaboradores que se requiere de la validación del ambiente de trabajo y ubicación física mediante el uso de tomas de video, y que al menos antes de empezar las actividades diarias de trabajo, se deberá adelantar este registro. De igual forma, a manera de control, aleatoriamente se podrá solicitar a cualquier colaborador la realización de una validación con este método de captura de video cuando se considere necesario.

3. Construcción y Validación de ítems y Ensamble de Pruebas Escritas, construcción de casos y preguntas, formatos de evaluación y ensamble de pruebas especiales (Entrevista).		
3.2 Seguridad		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para Construcción y Validación de Ítems y Ensamble de Pruebas Escritas- Construcción de casos y preguntas, formatos de evaluación y ensamble de las pruebas especiales (entrevista)– Condiciones de Seguridad.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**

3.2.3	Control y Monitoreo	• La IES deberá mantener actualizados sus registros de colaboradores autorizados para la conexión remota en esta operación en contingencia. Dichos registros deben contar al menos con información acerca de:
		  • Equipo autorizado y revisado
		  • Tipo de rol o actividad del colaborador en el proceso
		  • Lista de accesos permitidos
		  • Franja horaria autorizada para operar por cada día.
		• La IES debe mantener actualizados los registros de configuraciones revisadas y últimos cambios realizados.
		• La IES deberá evidenciar el ajuste a sus políticas de toma de copias de seguridad de los repositorios de información, a las condiciones de operación en contingencia en donde se muestre que la frecuencia de ejecución y prueba ha aumentado.

3.2.4	Soporte	• La IES debe contar con una mesa de servicio, donde se registren los requerimientos de los colaboradores, generando un identificador único por cada requerimiento, registrar cada seguimiento y evidencias graficas de los servicios de apoyo a los equipos de los colaboradores. El inventario de PC de usuario final, equipos de las IES, dispositivos de comunicaciones, seguridad y demás componentes que formen parte de la solución tecnológica que soporta el proceso deben mantenerse actualizados, reportando cualquier novedad o cambio.
3.2.5	VPN Site-to-site	• La conectividad a la infraestructura de la CNSC debe contemplar la configuración de una VPN site-to-site, SSL, TLS o IPsec. Como esquema de contingencia de la CNSC debe configurarse apuntando a los dos proveedores de comunicaciones que tiene la entidad. • El tráfico permitido debe ser solo para las Vlan habilitadas y solicitadas por la IES, en lo posible con usuarios autenticados al dominio. • El equipo de seguridad firewall debe soportar VPN Ipsec.
3.2.6	Equipo de Seguridad Firewall Perimetral.	• El dispositivo de seguridad deberá soportar túneles de conexión segura para redes privadas virtuales (VPNs) con algoritmos de cifrado: AES, DES, 3DES en sus versiones más recientes. • Debe poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. • Se sugiere que el equipo firewall pueda estar en capacidad de definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Estos equipos deben soportar como mínimo una capacidad de 50 Gbps de Throughput, IPsec VPN Throughput 40 Gbps, SSL-VPN Throughput 3Gbps. Dichos portales deben poder asignarse de acuerdo con el grupo de pertenencia de dichos usuarios y mediante esta conexión y la VPN site-to.site alcanzar los recursos de la CNSC.

3. Construcción y Validación de ítems y Ensamble de Pruebas Escritas, construcción de casos y preguntas, formatos de evaluación y ensamble de pruebas especiales (Entrevista).		
3.3 Recurso Humano		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para Construcción y Validación de Ítems y Ensamble de Pruebas Escritas- Construcción de casos, preguntas, formatos de evaluación y ensamble de las pruebas especiales (entrevista) – Recurso Humano.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
3.3.1	Hojas de Vida	• Se debe realizar un estricto seguimiento a los perfiles profesionales contratados, almacenar dicha información en un lugar seguro en la IES.
3.3.2	Contratos	• Se debe almacenar con folio, todos los documentos que sean parte integral del contrato de cada uno de los colaboradores, junto a la hoja de vida.
3.3.3	Acuerdos de confidencialidad	• Se debe hacer firmar a cada uno de los colaboradores de la IES, acuerdos de confidencialidad, aclarando y entregando detalladamente al colaborador, las sanciones, multas y demás que se imponen, en caso de infringir dicho acuerdo. • La IES debe entregar, aclarar y socializar con el colaborador, los acuerdos de confidencialidad, con una vigencia no menor a un (1) año, a partir de la firma del contrato, donde se puede aplicar durante este tiempo sanciones, multas y demás, en caso divulgar, promocionar o mencionar, cualquier información inherente al objeto contractual.
3.3.4	Capacitación	• La IES debe realizar una jornada de sensibilización con todos los colaboradores autorizados para realizar trabajo a través de acceso remoto, sobre los controles dispuestos, las vulnerabilidades de este tipo de conexión, los mecanismos de control y monitoreo, las recomendaciones de seguridad aplicables. • La IES debe programar al menos una (1) vez al mes una capacitación, que abarque temas técnicos del uso de las herramientas para construcción de ítems, casos y preguntas y formatos de evaluación, buen uso de los equipos de cómputo y de aspectos legales y contractuales, que garanticen la seguridad, custodia y confiabilidad de la información. • Se debe evidenciar mediante encuesta el entendimiento de los colaboradores sobre el protocolo de solicitud de asistencia técnica y verificación del servicio prestado por la mesa de servicio autorizada por la IES.
3.3.5	Perfil Constructor	• Para el desarrollo de las actividades de trabajo remoto el constructor debe antes de iniciar labores diarias, hacer una grabación del sitio de trabajo con una vista de trescientos sesenta grados (360º), esta debe ser remitida al soporte tecnológico de la IES para que se archiven en un repositorio donde en cualquier momento se pueda consultar para labores de seguimiento por parte de la CNSC. • La cámara del computador o cámara externa si es el caso, debe estar siempre que el colaborador este trabajando, apuntando frente a él, de ninguna manera se pretende grabar lo que se esté visualizando en su pantalla.
	Perfil Validador	• Para el desarrollo de las actividades de trabajo remoto el grupo de colabores que esté haciendo la validación, si se reúnen virtualmente deben grabar solo el audio de la reunión y debe quedar en el repositorio que la IES haya definido para este fin, se debe poder asociar a qué ítem o ítems, casos y preguntas, se refería la reunión de validación. En cualquier momento estos audios pueden ser consultados para labores de seguimiento por parte de la CNSC, actividad que se organizará entre los ingenieros de apoyo asignados al proceso de selección por parte de la IES y la CNSC. • La elaboración de las actas de reuniones requeridas en el Anexo Técnico se mantiene.

3. Construcción y Validación de ítems y Ensamble de Pruebas Escritas, construcción de casos y preguntas, formatos de evaluación y ensamble de pruebas especiales (Entrevista).		
3.3 Recurso Humano		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para Construcción y Validación de Ítems y Ensamble de Pruebas Escritas - Construcción de casos y preguntas, formatos de evaluación y ensamble de las pruebas especiales (entrevista) – Recurso Humano.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
	Perfil Ensamblador	• Para el desarrollo de las actividades de trabajo remoto el ensamblador debe antes de iniciar labores diarias, hacer una grabación del sitio de trabajo con una vista de 360 grados y durante la ejecución de toda la actividad debe estar grabando, esta debe quedar en el repositorio seguro que la IES haya definido para este fin. En cualquier momento estos videos se pueden consultar para labores de seguimiento por parte de la CNSC, actividad que se organizará entre los ingenieros de apoyo asignados al proceso de selección por parte de la IES y la CNSC. • La cámara del computador o cámara externa si es el caso, debe estar siempre que el colaborador este trabajando, apuntando frente a él, de ninguna manera se pretende grabar lo que se esté visualizando en su pantalla. • Solo para este caso la IES puede determinar hacer este ensamble de pruebas en el sitio central a donde se conectar sus colaboradores, en cuyo caso deberá cumplir con las condiciones definidas en la opción 1 “Trabajo en Sitio”.

3. Construcción y Validación de ítems y Ensamble de Pruebas Escritas, construcción de casos y preguntas, formatos de evaluación y ensamble de pruebas especiales (Entrevista).		
3.4 Servicios		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para Construcción y Validación de Ítems y Ensamble de Pruebas Escritas - Construcción de casos y preguntas, formatos de evaluación y ensamble de las pruebas especiales (entrevista) – Servicios.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
3.4.1	Capacitación	• La IES debe realizar capacitación, llevando registro de asistencia, ya sea físico o virtual, donde explique y enseñe el uso de las herramientas tecnológicas con las que cuenta la universidad, para el trabajo, ya sea remoto o presencial. • La IES debe realizar la capacitación de las herramientas dispuestas para la construcción de ítems, casos y preguntas y formatos de evaluación, de acuerdo con los alcances contractuales entre la universidad y el colaborador, llevando registro de asistencia, ay sea físico o virtual. • La IES debe concientizar a manera de capacitación a cada uno de los colaboradores, y personas que de una u otra manera intervengan con la construcción de ítems, casos y preguntas y formatos de evaluación, ya sea personal de misión o de apoyo, sobre el manejo de la información, los niveles de confidencialidad de la información, de acuerdo con el marco de la norma ISO 27001 en su versión más reciente. Además, se debe especificar la clasificación y protección de la información aplicables al proceso, dejando de forma detallada que información es pública, cual es privada, cual es restringida, cual es confidencial y cual es secreta, así como la aplicabilidad de sanciones en la divulgación de la información, según el nivel.
3.4.2	Mesa de servicio	• La IES debe garantizar la disponibilidad de la mesa de servicio, durante el tiempo de conexión de los colaboradores, tanto de aplicación como de personal profesional de apoyo. • Los profesionales de apoyo para la mesa de servicio, debe ser personal exclusivo para el soporte a las personas en misión, ya sea de manera remota o presencial.
3.4.3	Horario de disponibilidad de la conexión remota	• La IES debe organizar los horarios de trabajo y deben ser coincidentes con la disponibilidad de la conexión remota, no se debe permitir ninguna conexión fuera del horario establecido. • El horario de conexión remota debe coincidir con el horario de la mesa de servicio.
3.4.4	Disponibilidad del servicio	• La IES debe garantizar la disponibilidad de los servicios, canales de internet, conexiones y gestión de mesa de servicio.

Sala para el Diseño de Cursos de Formación y Ensamble de la Evaluación Final de los Cursos de Formación.

Para el diseño de los Cursos de Formación y la Evaluación Final de los Cursos de Formación, bajo la opción de trabajo remoto la IES debe implementar una arquitectura tecnológica similar a la definida en el siguiente diagrama:

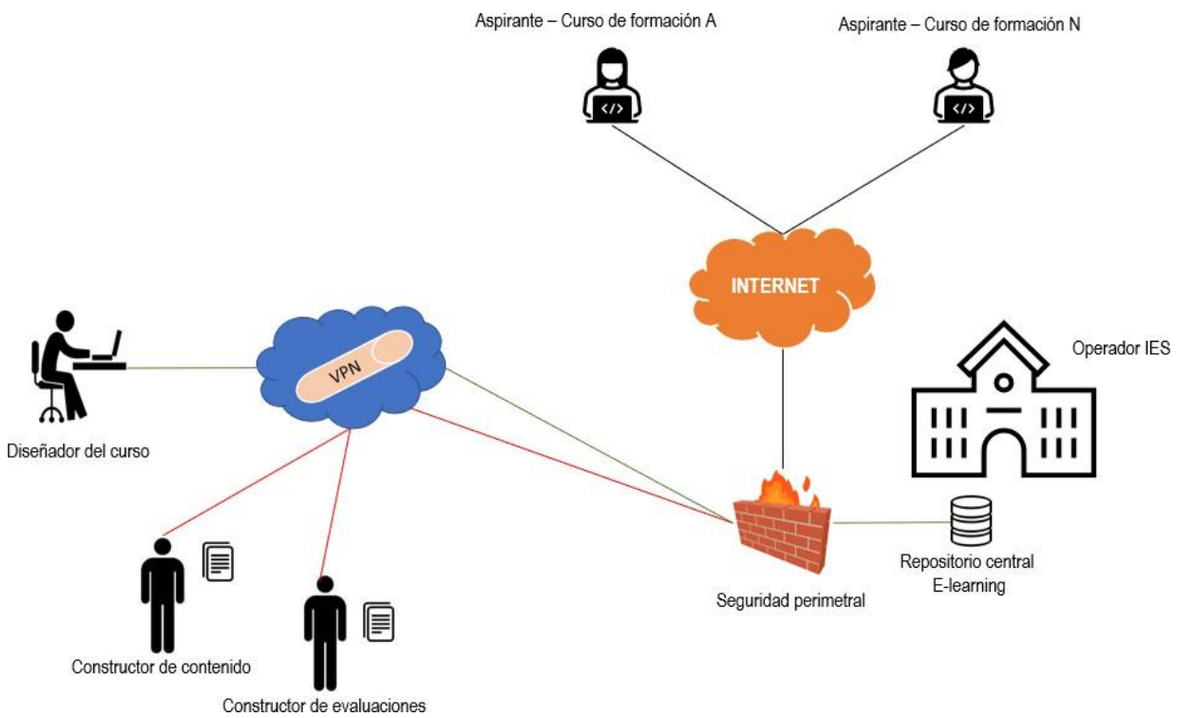


Ilustración 4. Esquema de conexión remota para el diseño de cursos de formación y ensamble de evaluación de los cursos de formación.

En este esquema, los colaboradores de la IES que operan bajo la modalidad de trabajo remoto, se conectan a través de un túnel seguro hacia el servicio de e-learning que está asegurado desde las instalaciones de la IES (por estar ubicado en sitio o por pertenecer a una lista blanca de accesos a los servicios de internet autorizados) para desarrollar las actividades de: Construcción del contenido de los cursos de formación, Construcción de los mecanismos de evaluación de los contenidos de los cursos y Diseñador general del curso y administrador de la plataforma de e-learning.

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.1 Comunicaciones		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**

4.1.1	Conexión remota	• Se debe garantizar que cada uno de los colaboradores de la IES cuente con un acceso remoto seguro y auditable a la infraestructura de la Institución de Educación Superior – IES. El nivel de auditoría por lo menos debe permitir observar: usuario conectado, fecha, hora de conexión y desconexión.
		
		• Siempre que se realice una conexión de escritorio remoto al equipo del colaborador esta deberá anunciársele con el fin de tener que esta no sea invasiva y altere su estado de privacidad.
		
		• El colaborador durante el desarrollo de su trabajo debe abstenerse de realizar actividades de carácter personal en el dispositivo de trabajo remoto destinado para el trabajo.
		Nota: el uso de smartphones está prohibido como terminal de trabajo remoto.
		
		• Si es posible habilitar una conexión con un segundo factor de autenticación la IES debe mantenerse este esquema durante la ejecución del contrato.
		
		• Configuración de registros automáticos revisables de:
		  • Administración de cuentas
		  • Inicios y cierre de sesión
		  • Acceso DC
		  • Acceso a objetos
		  • Uso de privilegios
		  • Sistema

4.1.2	Seguridad Remota	Cada acceso remoto debe configurarse de manera que el colaborador no pueda conectarse a ninguna otra red mientras esté utilizando la conexión remota de la IES.
		• Cada computador de los colaboradores debe ser inspeccionado remotamente por el personal técnico de la IES utilizando una herramienta tipo software de soporte remoto.
		
		• De forma automática, el sistema de autenticación deberá validar el cumplimiento de las características mínimas de seguridad de equipos o dispositivos de los colaboradores descritas en este numeral, para que permita la conexión remota.
		
		• El colaborador debe extremar las precauciones para evitar el acceso no autorizado a la información personal, propia y de terceros, manejada, no dejando a la vista ningún soporte de información en el lugar donde se desarrolle el trabajo remoto y bloqueando las sesiones de los dispositivos cuando estos estén desatendidos.
		
		• Cualquier anomalía que pueda afectar a la seguridad de la información debe notificarse al responsable del área de tecnología de la IES, a la mayor brevedad posible, a través de los canales definidos para el efecto.
		
		• Se debe contar con una configuración detallada de las de reglas de entrada y salida del cortafuegos (lógico o físico) de la IES.
		  • Acciones: permitir o bloquear
		  • Protocolos IP
		  • Direcciones IP entrada / salida

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.1 Comunicaciones		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
4.1.3	Equipos o dispositivos de los colaboradores	• El colaborador debe contar con una conexión a internet en su lugar de residencia, con un operador reconocido en el mercado colombiano, avalado por el ministerio de las tecnologías de la información y las comunicaciones (MINTIC). • La IES debe validar que la conectividad del equipo se realice mediante una conexión segura de internet, en lo posible usar conectividad cableada y que el equipo o dispositivo del colaborador tenga la red inalámbrica deshabilitada. • Se recomienda que la velocidad mínima contratada por el colaborador con el operador o ISP sea al menos de 10Mbps. • En caso de autorizar una política de BYOD para realizar las actividades de diseño y ensamble de la evaluación final de los cursos de formación, el colaborador debe: a. Aceptar la instalación de las herramientas necesarias para el control y soporte remoto dispuestos por la IES. b. Comprometerse a no usar repositorios locales (disco duro fijo, memorias o discos extraíbles) para la construcción de documentos intermedios de gestión o para realizar localmente la validación de los archivos vinculados por los aspirantes que están relacionados con el proceso de selección. c. Conceder derechos de revisión del contenido de los repositorios de almacenamiento de información locales, por parte de los supervisores del contrato o por cualquier proceso de auditoría que adelante la CNSC para validar el avance de las actividades del cronograma propuesto por la IES para esta etapa. d. Acogerse a las medidas de control, monitoreo y revisión que la IES adopte para los dispositivos aportados al proceso como si fuese parte del inventario de equipos administrados por la IES. e. Permitir el acceso remoto para realizar actividades de borrado seguro de los contenidos, archivos o datos que la mesa de ayuda de la IES identifique como información relacionada con el proceso de selección con el cual está vinculado.
4.1.4	Registros automáticos de control (Logs) y auditoría	• Se debe llevar un registro detallado de hora, fecha, dirección IP origen y usuario que se ha conectado al acceso remoto. • Se debe llevar una bitácora de revisión de cumplimiento de los requisitos mínimos de los equipos de los colaboradores. • La IES debe programar revisiones aleatorias diarias, para validar el cumplimiento de las condiciones mínimas de operación de los equipos o dispositivos de los colaboradores. La CNSC puede realizar auditoría en cualquier momento para verificar el cumplimiento de las condiciones, para lo cual el ingeniero designado por la CNSC contactará al ingeniero asignado por la IES y de esta manera coordinar la actividad. • Se debe llevar registro tipo checklist, por el personal técnico de la IES, donde detalle fecha y hora, nombre del colaborador revisado, nombre de la persona técnica que revisa el equipo, este registro debe ser digital y estar disponible en un repositorio para su consulta por parte de la CNSC.

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.1 Comunicaciones		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
4.1.5	Soporte	• La IES debe contar con una mesa de servicio, donde se registren los requerimientos de los colaboradores, generando un identificador único por cada requerimiento, registrar cada seguimiento y evidencias gráficas de los servicios de apoyo a los colaboradores y a sus dispositivos de trabajo. • La IES debe contar con una herramienta de apoyo remoto de parte de la mesa de servicios que permita registrar el tipo de soporte dado, fecha y hora, de todos los servicios de apoyo que realiza esta mesa de servicio a los colaboradores.
4.1.6	Gestión de los Equipos de Conectividad	• La gestión de los equipos de comunicaciones debe realizarse mediante un protocolo de comunicaciones seguro y desde una Vlan en particular (Vlan de Gestión).
4.1.7	Interfaces de Conectividad	• Se requiere que el equipo de conectividad (Switch) cuente con interfaces de 1Gpbs/10Gbps, en lo posible Interfaces de 10 Gbps para la conexión con los equipos de seguridad perimetral – Firewall que debe soportar como mínimo una capacidad de 50 Gbps de Throughput, IPsec VPN Throughput 40 Gbps, SSL-VPN Throughput 3Gbps.

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.2 Seguridad		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación – Condiciones de Seguridad.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
4.2.1	Equipos o dispositivos de los colaboradores	• Debe contar con un sistema operativo soportado por el fabricante a la fecha de inicio de labores y compatible con la infraestructura software que implemente la IES. • Si el sistema operativo requiere licenciamiento, este debe ser licencia original emitida por el fabricante del hardware o del propio sistema operativo. • Para permitir conexión remota, se debe verificar y registrar por parte de la IES, en cada equipo o dispositivo del colaborador, las versiones de parches, hotfix o actualizaciones aplicadas correctamente a las últimas versiones liberadas por el fabricante. • El equipo o dispositivo del colaborador, debe contar con un sistema de antivirus reconocido, totalmente licenciado, se debe verificar y registrar por parte de la IES, las versiones de parches, hotfix o actualizaciones aplicadas correctamente a las últimas versiones liberadas por el fabricante. • El equipo o dispositivo del colaborador debe contar con un software de firewall, instalado y activo, se debe verificar y registrar por parte de la IES la funcionalidad del software de firewall. • Se debe generar una política de seguridad en el equipo del colaborador que, en el momento de establecer una conexión remota, se deshabiliten los puertos USB, unidades de CD, DVD, no se permita la redirección de dispositivos locales, ni a los equipos remotos en la IES. • Se debe permitir el establecimiento de una conexión de auditoría con el colaborador, donde se permita grabar y ver el entorno del colaborador, ya sea a través de la cámara web del equipo u otro mecanismo de grabación. • Para los casos en donde se autorice una política de BYOD el colaborador del proceso, que aporta su dispositivo personal debe: a. Evidenciar que se cumplen con las condiciones de licenciamiento de sistema operativo y aplicaciones requeridas para el cumplimiento de las tareas asignadas. b. Permitir a la IES que se acceda al dispositivo con plena autonomía para que se efectúen los controles y revisiones que la IES o la CNSC, considere necesarias. c. Abstenerse de compartir el dispositivo con otros usuarios durante el periodo durante el cual se adelanten las actividades indicadas por la IES sobre las cuales se autorizó el uso del mencionado dispositivo.

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.2 Seguridad		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación – Condiciones de Seguridad.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
4.2.2	Locación física del colaborador	• La IES debe velar, auditar y registrar, para que las condiciones, tanto físicas como ambientales, donde labora el colaborador, sea en un lugar aislado, cerrado, sin distractores, ni acompañantes y que, en caso de ser necesario, registrar por medio de video dicho entorno. • Se debe crear, aplicar y sensibilizar a los colaboradores sobre la política de NO uso de celular, tablets, relojes inteligentes o televisores, mientras se realizan las actividades propias del objeto contractual, y en lo posible, la universidad debe registrar y guardar dichas evidencias.

4.2.3	Control y Monitoreo	• La IES deberá mantener actualizados sus registros de colaboradores autorizados para la conexión remota en esta operación en contingencia. Dichos registros deben contar al menos con información acerca de:
		  • Equipo autorizado y revisado
		  • Tipo de rol o actividad del colaborador en el proceso
		  • Lista de accesos permitidos
		  • Franja horaria autorizada para operar por cada día.
		• La IES debe mantener actualizados los registros de configuraciones revisadas y últimos cambios realizados.
		• La IES deberá evidenciar el ajuste a sus políticas de toma de copias de seguridad de los repositorios de información, a las condiciones de operación en contingencia en donde se muestre que la frecuencia de ejecución y prueba ha aumentado.

4.2.4	Soporte	• La IES debe contar con una mesa de servicio, donde se registren los requerimientos de los colaboradores, generando un identificador único por cada requerimiento, registrar cada seguimiento y evidencias graficas de los servicios de apoyo a los equipos de los colaboradores. • El inventario de PC de usuario final, los de las IES, equipos de comunicaciones, seguridad y otros que formen parte de la solución tecnológica que soporta el proceso deben mantenerse actualizado, reportando cualquier novedad por cambio.
4.2.5	VPN Site-to-site	• La conectividad a la infraestructura de la IES debe contemplar la configuración de una VPN site-to-site, SSL, TLS o Ipsec que incluya esquemas de contingencia a cualquiera de los proveedores de comunicaciones que tiene la IES. • El tráfico permitido debe ser solo para las Vlan habilitadas y solicitadas por la IES, en lo posible con usuarios autenticados al dominio. • El equipo de seguridad firewall debe soportar VPN Ipsec.

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.2 Seguridad		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación – Condiciones de Seguridad.**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
4.2.6	Equipo de Seguridad Firewall Perimetral.	• El dispositivo de seguridad deberá soportar túneles de conexión segura para redes privadas virtuales (VPNs) con algoritmos de cifrado: AES, DES, 3DES en sus versiones más recientes. • Debe poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. • Se sugiere que el equipo firewall pueda estar en capacidad de definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Estos equipos deben soportar como mínimo una capacidad de 50 Gbps de Throughput, IPsec VPN Throughput 40 Gbps, SSL-VPN Throughput 3Gbps. Dichos portales deben poder asignarse de acuerdo con el grupo de pertenencia de dichos usuarios.

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.3 Recurso Humano		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación– Condiciones relacionadas con el Talento Humano**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
4.3.1	Hojas de Vida	• Se debe realizar un estricto seguimiento a los perfiles profesionales contratados, almacenar dicha información en un lugar seguro en la IES.
4.3.2	Contratos	• Se debe almacenar con folio, todos los documentos que sean parte integral del contrato de cada uno de los colaboradores, junto a la hoja de vida.
4.3.3	Acuerdos de confidencialidad	• Se debe hacer firmar a cada uno de los colaboradores de la IES, acuerdos de confidencialidad, aclarando y entregando detalladamente al colaborador, las sanciones, multas y demás que se imponen, en caso de infringir dicho acuerdo. • La IES debe entregar, aclarar y socializar con el colaborador, los acuerdos de confidencialidad, con una vigencia no menor a un (1) año, a partir de la firma del contrato, donde se puede aplicar durante este tiempo sanciones, multas y demás, en caso divulgar, promocionar o mencionar, cualquier información inherente al objeto contractual.
4.3.4	Capacitación	• La IES debe realizar una jornada de sensibilización con todos los colaboradores autorizados para realizar trabajo a través de acceso remoto, sobre los controles dispuestos, las vulnerabilidades de este tipo de conexión, los mecanismos de control y monitoreo, las recomendaciones de seguridad aplicables. • La IES debe programar al menos una (1) vez al mes una capacitación, que abarque temas técnicos del uso de las herramientas para construcción de ítems, buen uso de los equipos de cómputo y de aspectos legales y contractuales, que garanticen la seguridad, custodia y confiabilidad de la información. • Se debe evidenciar mediante encuesta el entendimiento de los colaboradores sobre el protocolo de solicitud de asistencia técnica y verificación del servicio prestado por la mesa de servicio autorizada por la IES.
4.3.5	Perfil Constructor de contenido de los Cursos de Formación	• Para el desarrollo de las actividades de trabajo remoto el constructor del contenido del curso debe antes de iniciar labores diarias, hacer una grabación del sitio de trabajo con una vista de trescientos sesenta grados (360º), esta debe ser remitida al soporte tecnológico de la IES para que se archiven en un repositorio donde en cualquier momento se pueda consultar para labores de seguimiento por parte de la CNSC. • La cámara del computador o cámara externa si es el caso, debe estar siempre que el colaborador este trabajando, apuntando frente a él, de ninguna manera se pretende grabar lo que se esté visualizando en su pantalla.
	Perfil Constructor de evaluaciones de los Cursos de Formación	• Para el desarrollo de las actividades de trabajo remoto el grupo de colabores que esté haciendo construcción de las evaluaciones del curso de formación debe antes de iniciar labores diarias, hacer una grabación del sitio de trabajo con una vista de trescientos sesenta grados (360º), esta debe ser remitida al soporte tecnológico de la IES para que se archiven en un repositorio donde en cualquier momento se pueda consultar para labores de seguimiento por parte de la CNSC. • Debe abstenerse de adelantar cualquier tipo de grabación de audios, videos o capturas de pantalla de las evaluaciones totales o parciales que se hayan definido para los cursos de formación del proceso de selección.

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.3 Recurso Humano		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación – Condiciones relacionadas con el Talento Humano**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
	Perfil Diseñador de los Cursos de Formación	• Para el desarrollo de las actividades de trabajo remoto el Diseñador del Curso de Formación debe antes de iniciar labores diarias, hacer una grabación del sitio de trabajo con una vista de 360 grados y durante la ejecución de toda la actividad debe estar grabando, esta debe quedar en el repositorio seguro que la IES haya definido para este fin. En cualquier momento estos videos se pueden consultar para labores de seguimiento por parte de la CNSC, actividad que se organizará entre los ingenieros de apoyo asignados para el proceso de selección por parte de la IES y la CNSC. • La cámara del computador o cámara externa si es el caso, debe estar siempre que el colaborador este trabajando, apuntando frente a él, de ninguna manera se pretende grabar lo que se esté visualizando en su pantalla. • Para este perfil la IES puede determinar si se puede hacer este diseño del curso en el sitio central a donde se conectar sus colaboradores, en cuyo caso deberá cumplir con las condiciones definidas en la opción 1 “Trabajo en Sitio”.
	Perfil Diseñador	• Para el desarrollo de las actividades de trabajo remoto el diseñador debe establecer la conexión remota a través del canal aprobado, realizando todas las tareas de diseño, revisión y ajuste del material de los Cursos de Formación, ya sea a nivel de contenido temático, diseño pedagógico o diseño instruccional, manejando la información relacionada con las unidades de aprendizaje y los contenidos temáticos de forma exclusiva por este medio.
	Perfil Virtualizador	• Para el desarrollo de las actividades de trabajo remoto el virtualizador debe establecer la conexión remota a través del canal aprobado y hacer uso de los aplicativos destinados para las labores relacionadas con la diagramación del contenido del curso, la traducción de los elementos del curso al lenguaje requerido para el cargue en la plataforma virtual y posterior cargue del contenido.

4. Diseño y Evaluación Final de los Cursos de Formación.		
4.4 Servicios		
DENOMINACIÓN TÉCNICA:		**Conexión remota a la IES para el Diseño y Ensamble de la Evaluación Final de los Cursos de Formación– Servicios relacionados**
ÍTEM	**CARACTERÍSTICA**	**MÍNIMO REQUERIDO**
4.4.1	Capacitación	• La IES debe realizar capacitación, llevando registro de asistencia, ya sea físico o virtual, donde explique y enseñe el uso de las herramientas tecnológicas con las que cuenta, para el trabajo, ya sea remoto o presencial. • La IES debe realizar la capacitación de las herramientas dispuestas para el diseño, publicación y evaluación de los cursos de formación en la plataforma de e-learning autorizada de acuerdo con los alcances contractuales entre la IES y el colaborador, llevando registro de asistencia, bien sea en el modelo físico o virtual. • La IES debe concientizar a manera de capacitación a cada uno de los colaboradores, y personas que de una u otra manera intervengan con el diseño, publicación y evaluación de los cursos de formación en la plataforma de e-learning autorizada, ya sea personal de misión o de apoyo, sobre el manejo de la información, los niveles de confidencialidad de la información, de acuerdo con el marco de la norma ISO 27001 en su versión más reciente. Además, se debe especificar la clasificación y protección de la información aplicables al proceso, dejando de forma detallada que información es pública, cual es privada, cual es restringida, cual es confidencial y cual es secreta, así como la aplicabilidad de sanciones en la divulgación de la información, según el nivel.
4.4.2	Mesa de servicio	• La IES debe garantizar la disponibilidad de la mesa de servicio, durante el tiempo de conexión de los colaboradores, tanto de aplicación como de personal profesional de apoyo. • Los profesionales de apoyo para la mesa de servicio, debe ser personal exclusivo para el soporte a las personas en misión, ya sea de manera remota o presencial.
4.4.3	Horario de disponibilidad de la conexión remota	• La IES debe organizar los horarios de trabajo y deben ser coincidentes con la disponibilidad de la conexión remota, no se debe permitir ninguna conexión fuera del horario establecido. • El horario de conexión remota debe coincidir con el horario de la mesa de servicio.
4.4.4	Disponibilidad del servicio	• La IES debe garantizar la disponibilidad de los servicios, canales de internet, conexiones y gestión de mesa de servicio.

ACEPTACIÓN DE LOS ACUERDOS DE LOS NIVELES DE SERVICIO DE LA INFRAESTRUCTURA TECNOLÓGICA

En calidad de representante legal de la _____ (escriba el nombre de la Universidad o Institución de Educación Superior proponente), manifiesto que **ACEPTO LOS NIVELES DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES Y DE SEGURIDAD FÍSICA Y LÓGICA** descritos en la opción _____ (___) exigidos para la automatización de la información del proceso de selección, y en caso de resultar seleccionado, me comprometo a dar cumplimiento a las condiciones suscritas en el Anexo No. 9 bajo la opción seleccionada la cual mantendré durante la ejecución del contrato.

_____

NOMBRE Y FIRMA REPRESENTANTE LEGAL