CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA :DIGITAL

TELETRABAJO Y LA SEGURIDAD DE ACCESO REMOTO

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Fecha de publicación: 19 de marzo de 2020

© Todos los derechos reservados

INTRODUCCIÓN

El Centro Nacional de Ciberseguridad de la República Dominicana, a través del Equipo Nacional de Respuesta a Incidentes Cibernéticos CSIRT-RD, pone a disposición de la comunidad objetivo, empresarios y ciudadanos en general, esta guía para el uso correcto y buenas prácticas de la modalidad teletrabajo o trabajo remoto y el uso adecuado de las herramientas tecnológicas para garantizar la confidencialidad, integridad y disponibilidad de las informaciones que estarán siendo manejadas por los usuarios desde otra localidad de trabajo distinto a la empresa.

El **teletrabajo (trabajo remoto)** permite los empleados, contratistas, socios, comerciales, proveedores y otros usuarios de una organización realizar el trabajo desde ubicaciones remotas distintas a las instalaciones de la organización, a través de protocolos y herramientas de tecnología de la información y comunicación (TIC).

TELETRABAJO Y LA CIBERSEGURIDAD

Las soluciones de teletrabajo y acceso remoto necesitan cumplir varios objetivos de seguridad, los cuales se puede lograr con la aplicación de controles y herramientas tecnológicas integrados a los dispositivos y plataformas.

Los principios de seguridad para el teletrabajo y las tecnologías de acceso remoto son los siguientes:

- Confidencialidad: hay que asegurar que las comunicaciones de acceso remoto y los datos de usuarios almacenados no puedan ser accedidos por terceros no autorizados;
- Integridad: detectar cualquier cambio intencional o no intencional en las comunicaciones, servicios y datos de acceso remoto que se producen en tránsito;
- Disponibilidad: mantener disponible los recursos necesarios a través del acceso remoto al momento requerido por el usuario.
- Autorización: después de verificar la identidad de un usuario de acceso remoto, realizar verificaciones relacionadas con el dispositivo del cliente para determinar a qué recursos internos se debe permitir el acceso del usuario.

¿QUÉ TOMAR EN CUENTA AL MOMENTO DE REALIZAR EL TELETRABAJO?

Para las empresas

- Servidores de acceso remoto

Los servidores de acceso remoto deben colocarse en una zona desmilitarizada (también conocida como DMZ por sus siglas en ingles de Demilitarized Zone) de la organización para controlar las conexiones desde la red externa.

- Autenticación de acceso remoto, autorización y control de acceso

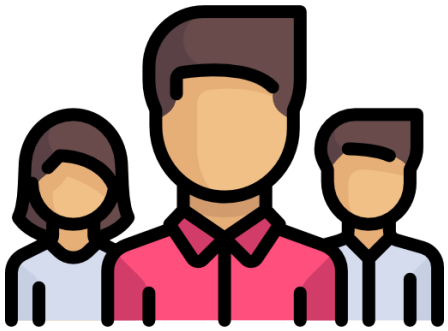
Los servidores de acceso remoto deben garantizar que el acceso esté restringido correctamente, autenticar cada usuario antes de otorgar acceso a los recursos de la organización y luego utilizar controles de autorización para garantizar que solo se puedan utilizar los recursos necesarios.

Entre las características mínimas que debe cumplir las tecnologías de autorización se encuentran las siguientes;

- Zero Trust: marco de seguridad basado en un proceso estricto de verificación de identidad que establece que solo los usuarios y dispositivos autenticados autorizados pueden acceder a las aplicaciones y datos.
- Control de acceso para comunicaciones de red: un componente importante para controlar el acceso a las comunicaciones de red y proteger su contenido es el uso de la criptografía. Como mínimo, toda información confidencial que pase a Internet, redes inalámbricas y otras redes de acceso externo debe preservar la confidencialidad e integridad a través de recursos criptográficos.
- Clientes VPN: conexión de acceso remoto realizada por un usuario mediante una red privada que requiere autenticación para la comunicación. Algunas de las soluciones ofrecen la función de túnel dividido que canalizar todas las comunicaciones que involucran los recursos internos de la organización a través de la VPN, protegiéndolas, aumentando la eficiencia de las comunicaciones y reduciendo la carga, esta función le agrega más seguridad aquellos teletrabajadores que utilizan puntos de acceso no confiables.

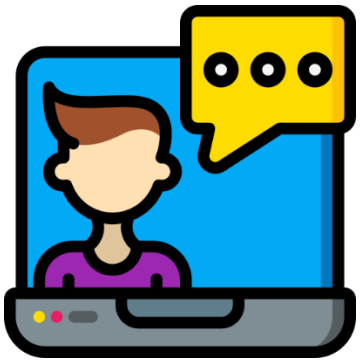
- **Seguridad del software del cliente de acceso remoto:** la entidad debe contemplar la realización de jornadas de mantenimiento remoto para aquellas aplicaciones que así lo requieran, con el objetivo de mantener las aplicaciones actualizadas y con los controles de seguridad adecuados.
- **MDM (Mobile Device Management:** la implementación de una plataforma corporativa de gestión de dispositivos móviles y es una buena medida para crear capacidades de control sobre las aplicaciones instaladas en los equipos de s usuarios remotos.

Para los usuarios finales



- Preferiblemente utilizar únicamente dispositivos provistos por la organización. No compartas estos equipos de trabajo con otras personas.
- Conéctate a los recursos de la organización a través de VPN, si no lo tiene implementa, evita utilizar redes públicas.
- Presta especial atención a los correos maliciosos, no abras mensajes o documentos adjuntos de dudosa o desconocida procedencia.
- Realiza periódicamente un respaldo externo de la información.
- Inhabilita los puertos USB y solo utiliza los recursos de compartir y almacenar archivos provisto por la organización.
- Utiliza doble factor de autenticación en todos los servicios en la nuble utilizados tanto para la gestión laboral como personal.
- Cifrar los discos duros es la mejor manera de proteger la información en caso de pérdida del equipo o intrusiones no autorizadas.
- Es importante el uso de antivirus.

VIDEOCONFERENCIAS



Las llamadas en conferencia y las reuniones web (reuniones virtuales) se constituyen en una herramienta del trabajo moderno. Desafortunadamente, si las reuniones virtuales no se configuran correctamente, personas externas podrían tener acceso una sesión de trabajo grupal. El uso de precauciones básicas puede ayudar a garantizar que las reuniones virtuales sean una oportunidad para colaborar y trabajar de manera efectiva, y no genere una violación de datos u otro incidente de seguridad o privacidad.

Independientemente del proveedor de plataforma, aquí hay algunas opciones para realizar una reunión virtual segura:

- Siga las políticas de su organización para la seguridad de las reuniones virtuales.
- Evite la reutilización de los códigos de acceso a las salas virtuales; si ha utilizado el mismo código durante un tiempo, probablemente haya sido compartido con personas externas.
- Si la videoconferencia es de carácter confidencial, use PIN únicos o códigos de identificación de la reunión, y considere la autenticación de doble factor.
- Si está disponible, use un panel de control para monitorear a los asistentes e identificar a todos los asistentes.
- No grabe la reunión a menos que sea necesario.
- Desactive las funciones que no necesita (como el chat, el intercambio de archivos o el video).
- Antes de que nadie comparta su pantalla, recuérdeles que no compartan otra información confidencial o personal durante la reunión sin darse cuenta.
- Solo realice reuniones web en dispositivos validados por la organización.