UNIVERSIDAD DEL BÍO-BÍO

Departamento de Servicios Computacionales

Guía para el

Teletrabajo UBB

Introducción

Introducción

El Teletrabajo o Teletrabajo remoto, es una modalidad en la cual el funcionario UBB puede realizar sus actividades profesionales fuera de la oficina.

Sin lugar a dudas esta metodología ha tomado gran fuerza debido a la situación actual en la que nos encontramos producto del COVID-19, e indudablemente esta quedará como alternativa ante la ocurrencia de futuros eventos.

La presente guía tiene como objetivo exponer todo el proceso y la relevancia que implica el teletrabajo, iniciando desde la solicitud y puesta en marcha del equipamiento que se utilizará, el acceso a la red corporativa, habilitación de servicios de conexión, instalaciones de software, permisos y cuidados sobre los equipos y software que se utilizarán. Además da a conocer las implicancias en la seguridad de los datos en términos de respaldo y la manipulación de información institucional vía servicios de accesos remotos, los cuales traen riesgos asociados debido a la naturaleza de las conexiones, por lo que como organización se deben establecer protocolos y pautas para evitar los riesgos asociados que esto trae como consecuencia.

Índice

01 Equipo utilizado

Equipo Utilizado

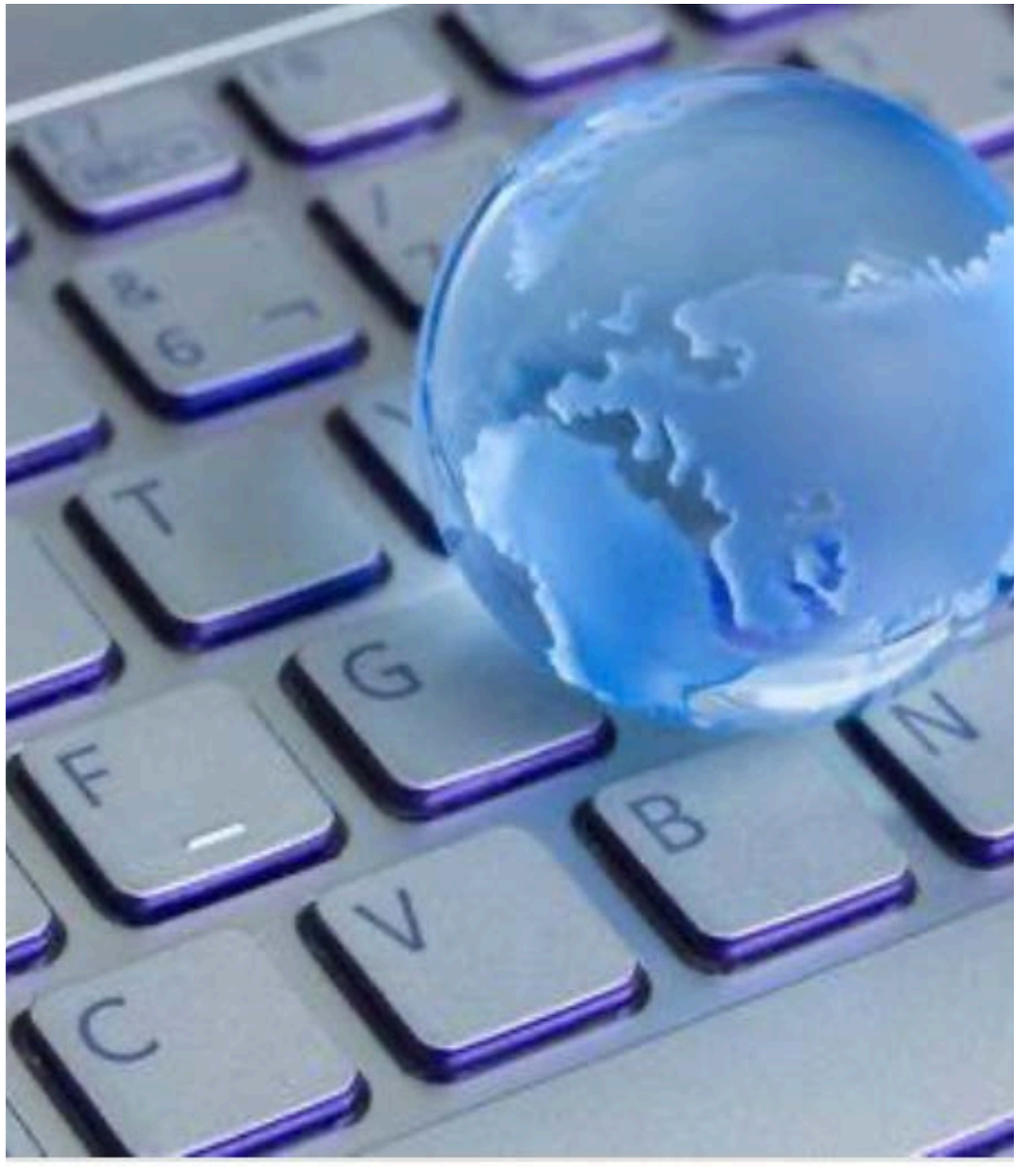
El equipamiento utilizado para el teletrabajo (trabajo remoto) es proporcionado por la universidad, incluyendo dentro de estos, equipos portátiles(Notebook) o los propios equipos(PC) que utiliza el funcionario dentro de la Universidad.

Este equipamiento puede ser configurado para el uso en teletrabajo mediante una conexión VPN. Es relevante mencionar que se prioriza la utilización y uso de equipamiento perteneciente a la universidad por temas tan vitales como lo son la seguridad de la información, seguridad de los datos, estandarización y normalización de softwares utilizados, licenciamiento y acceso a los sistemas corporativos (dominio), previendo o evitando los problemas que acarrean estos temas al instalarlos y habilitarlos en un equipo externo a la universidad, previniendo con esto riesgo que conlleva el uso de equipos propios debido al estado en términos de hardware y de software en el cual estos se puedan encontrar.

02 Acceso a la Red Corporativa UBB

Acceso a la red corporativa

Para el acceso a la red corporativa que involucra el acceso a sus servicios internos, tales como sistemas corporativos, acceso a entornos de desarrollo, administración de sitios web entre otros servicios disponibles, la universidad pone a disposición el acceso a sus redes corporativas mediante una Red Privada Virtual (VPN), la cual es instalada y habilitada en los equipos de los usuarios que lo requieran y solicitan.



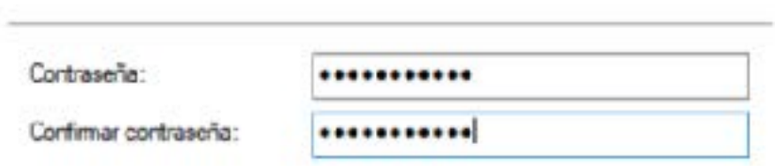
03 Habilitacion de VPN

Habilitación de VPN

Para la habilitación y configuración de la VPN, el usuario solicitante deben enviar un correo a operaciones@ubiobio.cl con copia a su jefatura y a soporte@ubiobio.cl, solicitando la habilitación de su cuenta de dominio(usuario@ubiobio.cl) para acceso VPN.

La habilitación y configuración del software de la VPN la realiza el área de soporte de la Dirección de Informática en el equipo que es utilizado por el usuario para el teletrabajo.

04 Uso de cuentas corporativas



Cuidados asociados a su uso

El cuidado en el uso de las cuentas corporativas tiene directa relación con la privacidad y seguridad que se debe mantener sobre los datos de la cuenta, en particular de la contraseña. En relación a lo señalado se recomienda lo siguiente:

- Nunca entregar nombre de usuario y mucho menos la contraseña a otra persona.
- Cambiar con regularidad la contraseña, idealmente cada tres meses.
- Utilizar contraseñas que no incluyan datos del usuario, como cumpleaños, parte del nombre o términos que el usuario tenga de uso regular y conocido por otras personas.
- Utilizar siempre caracteres variados, como por ejemplo . / _ * %, etc.
- Nunca dejar la contraseña registrada en papel.
- No entregar datos de la cuenta y/o contraseñas solicitados por correo.

Seguridad y accesos

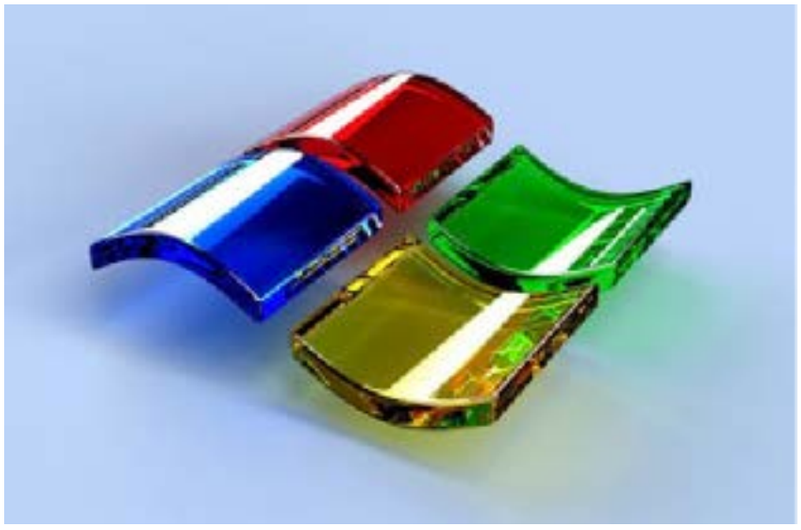
- No compartir sus contraseñas, son el único medio que acredita quién es la persona que está ejecutando la acción, por lo que esta debe ser uso personal e intransferible.
- Iniciar sesión solo en dispositivos confiables y no en lo posible no de terceros, ya que su cuenta puede verse comprometida/afectada por un entorno no actualizado(sistema operativo), poco resguardado o en el peor de los casos comprometido.
- Es conveniente tener más de un medio de autenticación. La seguridad de su cuenta no solo debe contar con una contraseña, siempre se recomienda tener al menos dos tipos o formas de autenticación para el uso de sus cuentas (correo secundario, mensaje al celular, reconocimiento biométrico, etc).
- Siempre es muy recomendable tener habilitada al menos una opción de notificaciones de inicio de sesión, actividad o modificaciones a la misma.

Mantención de cuentas

Dentro del mantenimiento de su cuenta se recomienda:

- Conocer la contraseña de su cuenta, de lo contrario usted la puedes recuperar ingresando en el portal de autogestión institucional de contraseña en el sitio https://idubb.ubiobio.cl/pwm
- Se recomienda renovar la contraseña cada tres meses como máximo.
- Verificar la información contenida en su perfil institucional, ingresando a https://myaccount.google.com/, con su cuenta “usuario”@ubiobio.cl
- Se recomienda revisar el apartado de “seguridad” en el perfil de su cuenta de correo UBB, en el cual encontrara información referente a la actividad de su cuenta, métodos para verificar su identidad, dispositivos asociados, entre otros.

05 Actualización de herramientas de uso diario



Sistema Operativo
La actualización del sistema operativo es una prioridad sobre la seguridad en el uso diario del equipo, por lo anterior se debe tener en consideración las advertencias que entrega el sistema operativo respecto a estas actualizaciones y aplicarlas con la regularidad sugerida.
Si por motivos de configuración inicial las actualizaciones no se realizan en forma automática estas deben ser revisadas y aplicadas a lo menos una vez por semana, ya que con esto se previenen las posibles fallas de seguridad producto del sistema operativo y el correcto funcionamiento del equipo.

Antivirus
Otra de las herramientas a la cual se debe prestar atención es la correcta y periódica actualización del antivirus corporativo ESET NOD32 que posee la universidad.
Este al igual que el sistema operativo, se actualiza en forma automática reportando el mismo software el éxito o falla de dicho proceso. En el caso de falla se debe reportar mediante correo electrónico a soporte@ubiobio.cl para que sea revisado.

Otros software
Los software que están instalados en los equipos, ya sea ofimática, software de especialidad no requieren actualizaciones frecuentes, solo podrían requerir soporte por fallas en su funcionamiento o por alguna actualización crítica que deba ser aplicada.
Todo el software instalado en los equipos debe estar debidamente licenciado y actualizado y está sujeto a revisión por parte de la Dirección de Informática conforme a lo indicado y expuesto en el decreto 3060 del 10 de septiembre de 2013.

06 Respaldo de datos y seguridad de la información

Respaldo de datos

El respaldo de datos es una labor crítica a la cual se debe prestar atención y para lo cual la universidad pone a disposición el servicio de Google Drive para todos los funcionarios de la Universidad.

El respaldo de la información vía este medio es de responsabilidad exclusiva del usuario, el cual debe velar por efectuar respaldo de sus datos y asegurar su actualización periódica. Se recomienda en este sentido que el usuario utilice los recurso en-linea sin tener la necesidad de descargar los archivos en forma local y luego tener que volver a cargarlos a google drive.

Compartir datos

Google Drive permite compartir archivos con otros usuarios, permitiendo de esta forma el trabajo sobre el mismo archivo de un grupo de personas.

Para acceder a esta opción basta con compartir el recurso con el acceso definido por el usuario, es decir puede ser compartido sólo modo lectura o edición, lo cual dependerá del uso que se le requiera autorizar al resto de los usuarios. Nunca compartir para “todos” por que esto pone en riesgo el acceso al(los) recursos del usuario.

Seguridad de la Información

La seguridad sobre la información es critica y para ello la Dirección de Informática tiene establecida la Política de Servicios TI y Seguridad Informática, la cual tiene como objetivo de velar por el adecuado uso de los recursos tanto de hardware como de software de toda la comunidad Universitaria y que afectan directamente a la seguridad de la información.

Para mas antecedentes ver documento que se encuentra publicado en sitio de normalización(normalizacion.ubiobio.cl), en documentos(procedimientos) del Depto de servicios Computacionales de la Dirección de Informática.

07 Identificar riesgos

Conexiones de red

Las conexiones de red disponibles en el equipo ya sea por medio de cable o vía conexión WIFI son un punto de entrada y causa de fallas de seguridad, nunca se debe conectar a redes publicas abiertas y mucho menos a aquellas que no posean contraseña de ingreso a la red o que tienen contraseñas publicas conocidas por todos. En ese sentido los riesgos de seguridad se pueden minimizar teniendo activo el cortafuego que trae el sistema operativo, procurando no acceder a sitios con advertencias de peligro de seguridad, manteniendo actualizado el sistema operativo y el antivirus.

Correos

La recepción de correos de origen no conocido o correos catalogados como Phishing, spam o correos con archivos adjuntos con extensiones .exe, .com, .bat o con extensiones desconocidas son causa de la mayoría de incidentes de seguridad. Con el fin de identificar este tipo de correos se recomienda:

- Ver quien emite el correo
- Su redacción suele ser muy básica y mal redactada.
- Contiene un “Asunto” sospechoso o no habitual.
- Contiene archivos adjuntos.
- Piden información y datos de la persona
- Contiene link adjuntos.
- Contienen información sobre caducidad de cuentas, eliminación o advertencias

Sitos Web

El acceso a sitios web sospechosos suelen ser advertidos hoy en día por todos los navegadores(browser). La detección de software malicioso y phishing está activada de forma predeterminada en la mayoría de los navegadores y al estar habilitada esta opción es posible que aparezcan los siguientes mensajes, por lo que si aparece alguno de ellos, te recomendamos que no accedas al sitio web.

Estos mensajes son:

- El sitio web al que vas a acceder contiene software malicioso, engañoso o contiene programas dañinos.
- Sitio web sospechoso
- Esta página está intentando cargar scripts de fuentes no autorizadas
- ¿Querías decir [nombre del sitio web]?