Grant Thornton

Auditoria

Normatividad

Global

Recomendaciones de seguridad de temas tecnológicos en estos tiempos de contingencia

La tecnología juega un papel importante para mantener nuestros negocios a flote durante esta contingencia. Es importante utilizarla de manera correcta y con las medidas de seguridad necesarias, ya que omitir dicha seguridad puede perjudicar comprometiendo información, activos de la entidad y clientes.

Para trabajar a distancia o en línea y con el propósito de seguir laborando sin comprometer el recurso humano (que es el recurso más importante de cualquier entidad), el primer paso sin duda es la selección de los sistemas principales, aquellos que son vitales para el negocio, así como el personal específico para laborar, para este proceso es necesario:

- Identificar los sistemas vitales de la entidad (que sean necesarios para seguir operando), refiriéndose a aquellos donde la producción, contabilidad, cobranza y venta se detienen en su ausencia.
- Identificar el personal que tiene mayores privilegios sobre estos sistemas, ya que estos serán los que continuarán laborando desde casa.
- Identificar y configurar los accesos remotos que el personal debe tener en cada uno de los sistemas, es decir cómo se van a conectar desde casa a los sistemas. La configuración debe identificar redes privadas virtuales (VPN), protocolos de comunicación seguros y sobre todo puertos de comunicación seguros.

Este punto de configuración de accesos remotos dependerá completamente de la infraestructura que se tenga, tomando en cuenta dos escenarios:

- El primero y más complejo es aquel donde la entidad cuenta con un site y servidores bajo sus instalaciones, en este caso la configuración deberá ser más robusta.
- Para el segundo escenario es para cuando se tiene todo en la nube en este caso la configuración será más facial ya que será similar a la que ya se tiene en la empresa.

Una vez identificados los elementos, así como la forma de comunicación, se deberá realizar la selección de los equipos computo para poder conectarse; esto no es menos importante ya que estos serán los medios de comunicación y en su caso serán los objetivos de cualquier atacante, por eso es recomendable que los equipos sean proporcionados por la entidad con configuraciones específicas. Si la entidad no puede proporcionar equipos, estará obligada a que, si el personal se encuentra en disposición de hacer home office, debe revisar el equipo con el que se conectará para que cuente por lo menos con:

- Bloqueo de puertos y servicios innecesarios (solo puertos seguros)
- Instalación de un software de antivirus que este siempre actualizado

- Instalación de un software antimalware
- Desinstalar programas que permitan conexiones P2P (punto a punto) para descargas tales como: Torrents, Vuze, uTorrent, etc.
- Una buena solución, es la instalación de filtro de contenido para páginas web esto evitara que los usuarios no tengan acceso a paginas peligrosas o en su defecto a páginas que quiten el tiempo en horas de trabajo incluso páginas de redes sociales.

Una vez realizadas las identificaciones y configuraciones, es importante solicitar al personal el ambiente de trabajo, es decir, solicitar una red de casa segura. Esta red no debe utilizar un protocolo de seguridad WEP en la red WIFI. Sobre todo, que el personal no deberá imprimir y tirar a la basura información confidencial de la entidad o del cliente, así como no exponer cualquier información en redes sociales.

En caso de reuniones virtuales, es importante manejar los códigos de accesos y URL's (direcciones de acceso) de manera adecuada y segura, así como no divulgarlos, ya que se puede tener acceso a personal no invitado. Por ende, también se sugiere que el administrador controle los accesos a la sala para garantizar que solo entra el personal invitado. De igual forma, la grabación de estas reuniones, así como la publicación de las imágenes de esta, debe ser con el permiso de todos los participantes ya que pudieran caer en un delito o en su defecto si no se cuidan las imágenes revelar información privada (gráficos, datos, cuentas o protocolos de seguridad).

No importa cuanta configuración o medios de seguridad de sistemas se tengan o se utilicen, todos estos tendrán una debilidad en caso de que el usuario no sea consciente de la seguridad y la importancia de la información que maneja, por eso los cursos para fomentar y concientizar la seguridad en los usuarios son esenciales e importantes.

Cualquier duda o apoyo que requieran no duden en comunicarse con nuestros especialistas.

Si desea más información o apoyo sobre cualquiera de los temas abordados por favor contáctenos.

Los asesores de Grant Thornton están enfocados en trabajar junto a nuestros clientes para apoyarlos en estos tiempos desafiantes de condiciones operativas críticas.

Roderick Marquis
Audit Partner
Grant Thornton Venezuela
E roderick.marquis@ve.gt.com

Jorge Gómez
Audit Partner
Grant Thornton Venezuela
E jorge.gomez@ve.gt.com

Carlos Diaz
Tax Partner
Grant Thornton Venezuela
E carlos.diaz@ve.gt.com

Grant Thornton

www.grantthornton.com.ve/