auren

#QuédateEnCasa

www.auren.com

Ciberseguridad y Tecnología

Contexto

Desde el punto de vista TIC el estado alarma por COVID-19 ha supuesto:

- Uso masivo del teletrabajo
- Uso de videoconferencias para suplir las reuniones presenciales
- Incremento exponencial de contratación on-line
- La presencia en redes sociales es clave para la imagen
- Las nuevas tecnologías (Ej: big data) pueda ayudar a identificar la nueva demanda u ofrecer servicios más personalizados
- Incremento de los ataques por uso masivo de tecnologías de la información y poca preparación frente al actual escenario remoto imprevisto en muchos casos.

Sin la digitalización y securización de sus procesos y actividades las empresas no podrán sobrevivir a esta situación, que podrá repetirse nuevamente en caso de un nuevo repunte.

Vectores de Actuación y Mejora

Las acciones a acometer por parte de las organizaciones se agrupan en los siguientes vectores o líneas de actuación:

Sistemas y Aplicaciones	Redes y Comunicaciones	Procesos y Procedimientos

Sistemas y aplicaciones

- Ampliación o redimensionamiento de la población de equipos móviles y/o portátiles corporativos
- Securización de dispositivos móviles y/o portátiles, corporativos o políticas estrictas BYOD (Bring Your Own Device).
- En su caso, adaptación de las actuales infraestructuras para poder operar remotamente en aquellos sistemas y aplicaciones que se determinen.
- Análisis de capacidad y carga de los actuales sistemas hardware para el trabajo remoto (o capacidad de los proveedores) tanto las aplicaciones corporativas como web y e-commerce.
- Evaluación de la seguridad y cumplimiento de los mecanismos actuales de comunicación corporativa o previa a su contratación (correo electrónico, chat, mensajería, video-conferencia, streaming, etc.) bien sean móviles (apps o pc) o aplicaciones de pago por uso en proveedores en cloud (Software as a Service)

Redes y Comunicaciones

- Revisión y mejora en su caso del ancho de banda y capacidad de las redes de comunicaciones tanto a nivel de las sedes corporativas y como CPDs
- Contratación en su caso de conexiones y proveedores de red y telefonía alternativos
- Revisión de necesidades y en su caso contratación de soluciones de conectividad en hogares de personas clave (router 4G, fibra óptica, etc.), así como securizar la instalaciones de los hogares del personal sensible (router local)
- Revisión del nivel de seguridad de las redes corporativas y recursos externos (hacking ético) al incrementarse el número de servicios publicados al exterior y en algún caso flexibilizarse reglas de acceso.
- Revisión y mejora de los sistemas de conexión remota (VPNs) y su capacidad en concurrencia (licencias, carga CPU, etc.)
- Revisión de reglas y configuración, así como de la capacidad y correcta operación (o contratación en su caso) de los los sistemas de monitorización y de seguridad perimetral (activa o pasiva) de las redes corporativas, así como de los mecanismos de registro de eventos.

Procesos y procedimientos

- Análisis o revisión en su caso de las TIC que soportan los procesos críticos TIC (Business Impact Analysis)
- Revisar, redefinir y mejorar sus planes de contingencia TIC y sus escenarios, especialmente el de pandemias (en base a las lecciones aprendidas tras este primer mes de estado de alarma)
- Políticas y procedimientos para el control de la información en las comunicaciones, marketing y redes sociales (interna y externa) – categorización de la información
- Reforzar los procedimientos de autorización (pagos, altas de usuario, cambios, etc.)
- Incorporaciones de soluciones de firma electrónica – securizando adecuadamente las claves
- Formación y concienciación del personal (incluyendo simulaciones) frente a la mayor exposición a ciberataques (phishing suplantación de identidad, fraude del CEO, etc.), buen uso de los equipos corporativos y medios de comunicación (email, videoconferencia, apps, chats, etc.)