TRAIN FOR TRADE

UNITED NATIONS
UNCTAD

Curso de Puertos Resilientes ante las Pandemias

Manual del participante
Sección 3 – Preparación tecnológica

Fortalecimiento de los conocimientos
y habilidades a través de enfoques innovadores
para el desarrollo económico sostenible

Development Account
Department of Economic and Social Affairs

Irish Aid
Government of Ireland
Rialtas na hÉireann

learn.unctad.org

Table of Contents

3.1 Tecnología, capacidad y seguridad del teletrabajo 1
3.2 Herramientas de productividad en el teletrabajo..... 6
3.3 Dejando de utilizar el papel 9
3.4 Seguridad y resiliencia informática 11

Copyright @ Naciones Unidas 2022
Todos los derechos reservados

Foto: Tom Fisk / Pexel

3. PREPARACIÓN TECNOLÓGICA

Los recursos tecnológicos (aplicaciones, procesos, sistemas de información y comunicación) suelen estar diseñados para su uso en circunstancias y condiciones normales. A continuación, se presentan algunos ejemplos de decisiones de diseño que suelen tomarse en circunstancias normales:

- Los principales sistemas de información de la empresa sólo son accesibles a nivel local (desde la oficina a través de la red de área local corporativa, LAN) por razones de confidencialidad y seguridad.
- Aunque se ha avanzado y se sigue avanzando mucho en materia de digitalización y eliminación del papel, buscando de este modo una mayor eficiencia y respetando al medio ambiente, todavía hay muchos procesos que no se han digitalizado. En circunstancias normales, la digitalización de estos procesos se considera importante, aunque no urgente.
- En la mayoría de los casos, no se considera necesario implantar herramientas de colaboración, videoconferencia y teletrabajo debido a la presencialidad de la plantilla portuaria.
- El modo de trabajo in situ significa que, por lo general, los recursos de tecnología de la información (TI) que se ponen a disposición de los usuarios son dispositivos fijos (ordenadores de sobremesa) debido a la baja relación entre el coste y el rendimiento.
- Las líneas de comunicación (internas, externas y de Internet) se dimensionan y aseguran teniendo en cuenta los flujos de información (y los anchos de banda) que se requieren cuando la mayoría de los empleados trabajan de manera presencial.

Todas estas decisiones relativas al diseño pueden dejar de ser válidas en situaciones de pandemia, pudiendo volver a ser consideradas, diseñadas y priorizadas. La siguiente sección tratará de evaluar lo que se necesita para preparar los recursos tecnológicos a la hora de lidiar con una situación de pandemia.

Los objetivos de esta sección serán:

- Identificar soluciones tecnológicas apropiadas para acuerdos de trabajo alternativos;
- Planificar una transición sin papel;
- Identificar y aplicar herramientas de comunicación digital que sean eficaces.

3.1 Tecnología, capacidad y seguridad del teletrabajo

Los recursos tecnológicos se han diseñado en circunstancias normales, en las que el personal de la empresa suele realizar sus tareas de forma presencial desde el puesto de trabajo que se pone a su disposición y que incluye los dispositivos tecnológicos necesarios (ordenador personal o Tablet, impresora, entre otros). En una situación de pandemia, en la que las personas pueden verse en la obligación de permanecer aisladas en sus domicilios particulares, las organizaciones tienen que asegurarse de

UN Copyright © 2022

que los recursos necesarios estén disponibles de manera remota y de que tengan una capacidad suficiente.

En una situación de confinamiento, es necesario comprobar y adaptar los recursos tecnológicos para que:

- El personal disponga de los recursos necesarios para acceder a distancia a los sistemas de información de la empresa

  Debe garantizarse que todo el personal que trabaja a distancia disponga de los medios necesarios y suficientes para hacerlo. Los requisitos mínimos deben ser un ordenador y conexión a Internet disponibles en el lugar desde el que van a trabajar (por ejemplo, en casa).

  Como primer paso, es aconsejable elaborar una lista del personal que va a teletrabajar y desde dónde:

  √ Identificación, por parte del departamento de TI del puerto los empleados que disponen de un portátil que les permita trabajar a distancia.

  √ Cada empleado debe indicar si dispone de equipos propios (PC) y de una conexión a Internet de banda ancha WIFI o 4G/5G en el lugar donde se ubicaría su puesto de trabajo a distancia.

Política de un solo ordenador

Se recomienda que el puerto provea a los trabajadores con PCs para asegurar que están equipados con los mecanismos y medidas de seguridad corporativos (como los antivirus, política de actualización de parches de seguridad necesarios para una conexión segura a los sistemas de información). Por ello, es aconsejable adquirir los dispositivos necesarios para equipar a aquellos empleados que no dispongan de ellos, así como tener en cuenta la implantación de la política de ordenador único en la organización. Hasta la fecha, la mayoría de las empresas han proporcionado a los empleados un ordenador de trabajo en su puesto de trabajo habitual, complementándolo con un ordenador portátil sólo para aquellos que necesitaban tener movilidad debido a los requisitos de su trabajo.

En una situación de pandemia, el requisito de movilidad se amplía a toda la plantilla portuaria (o a la mayoría de ella). De este modo, ya no es necesario, salvo en casos excepcionales, que un usuario tenga dos ordenadores. Este es el sentido de una política de ordenador único: la organización proporciona a cada usuario sólo un ordenador portátil. En este sentido, la relación coste/rendimiento sigue siendo mejor para los ordenadores de sobremesa que para los portátiles, aunque la brecha se está reduciendo. Este hecho, junto con la necesidad de movilidad en caso de pandemia, la mayor seguridad de los equipos corporativos y la reducción de los costes de hardware y software en comparación con el mantenimiento de dos ordenadores, hace que la política de ordenador único sea algo que merezca la pena considerar y aplicar en las organizaciones.

En el caso de que para realizar las tareas de teletrabajo los empleados dispongan de un portátil personal en lugar de uno de la empresa, el equipo deberá cumplir unos requisitos mínimos tales como:

√ Tener instaladas las últimas actualizaciones del sistema operativo y de seguridad;

√ Tener instalado un antivirus actualizado.

UN Copyright © 2022

Además del hardware cada usuario debe tener una conexión a Internet de banda ancha WIFI. Si no es así, se deberán de adquirir conexiones 4G/5G ad-hoc, o la organización deberá comprobar si el empleado dispone de un teléfono móvil corporativo/personal con un plan de datos que permita compartir los datos con un ordenador y utilizarlo como conexión 4G/5G.

Además del PC y la conexión a Internet, es importante asegurarse de que los usuarios disponen del equipo necesario para poder teletrabajar. Por ejemplo, en el caso de las organizaciones que tienen un sistema de firma electrónica en sus procesos de gestión y disponen de un certificado digital en una tarjeta criptográfica, podría ser necesario proporcionar un lector de tarjetas criptográficas a los empleados que teletrabajan.

A modo resumen: es importante asegurarse de que todo el personal que va a trabajar a distancia disponga tanto de los recursos mínimos (PC y conexión a Internet de banda ancha) como de los recursos complementarios para acceder e interactuar con los sistemas de información empresarial de la organización. Para tal fin, un primer paso debería de ser establecer una lista y asegurarse de que todo el mundo está debidamente equipado.

- Los sistemas de información empresarial son accesibles desde fuera de la organización

Un segundo paso es asegurarse de que las aplicaciones y los servicios informáticos necesarios para realizar las funciones de los empleados que van a teletrabajar son accesibles desde fuera de la organización y que la experiencia del usuario es aceptable. Para tal fin, el tiempo de respuesta de los sistemas y aplicaciones debe ser el adecuado para que los empleados no se vean afectados de manera negativa por el acceso en modo remoto.

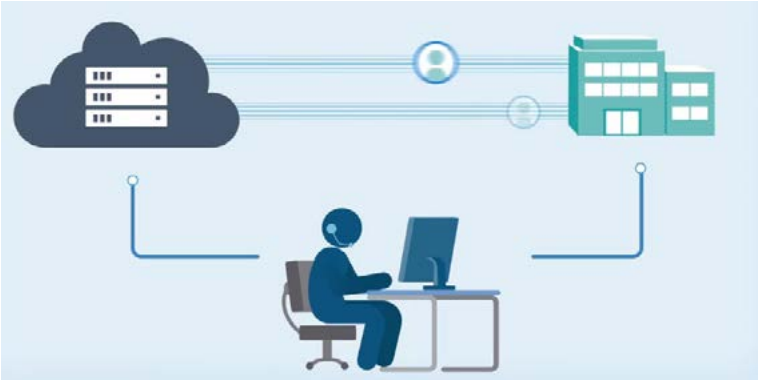
Por lo tanto, es necesario proporcionar los medios para que los sistemas corporativos sean accesibles y utilizables desde fuera de la organización. Para ello, hay que tener en cuenta los siguientes puntos:

a) Solución corporativa de acceso remoto

Una solución de acceso remoto permite establecer lo que se conoce como una VPN (red privada virtual) entre los dispositivos remotos y la red de la organización. De este modo, se crea una extensión segura (mediante el establecimiento de un túnel IPSec o SSL) de la red de área local (LAN) de la organización sobre una red pública y, en su defecto, de una insegura, como lo es Internet. Hay muchos fabricantes que ofrecen este tipo de solución. En caso de no estar disponible, se deben evaluar ambas alternativas (solución local o en la nube) para ver cuál es más adecuada dependiendo de las necesidades de la organización.

UN Copyright © 2022

Solución de acceso remoto a la nube



Si la organización aún no tiene instalada una solución de acceso remoto, podría plantearse una solución basada en la nube, que permite una implantación rápida y segura, incluso si la capacidad de la nube disponible en la organización es limitada. Este tipo de solución, ofrecida por muchos fabricantes en régimen de pago por uso, permite el acceso temporal a la organización desde cualquier lugar contando con las medidas de seguridad necesarias según el tipo de información que se maneje. Se basa en la transmisión de la capa de presentación de los sistemas corporativos a cualquier ordenador remoto siempre que se haya realizado la autenticación correspondiente. En este caso, se aísla completamente de la plataforma de acceso a la red corporativa, para evitar poner en riesgo los sistemas corporativos debido a las vulnerabilidades del cliente.

La arquitectura necesaria para proporcionar este tipo de acceso recae principalmente en la infraestructura utilizada por la nube. El usuario sólo necesita acceder a una página web para autenticarse y acceder a los servicios corporativos. La única parte de la arquitectura que es responsabilidad de cada organización es el despliegue de una pequeña máquina virtual, conocida como el "Connector", que establece una comunicación segura entre la nube y los servicios corporativos.

Independientemente del tipo de solución de acceso remoto elegido (en las instalaciones o en la nube), una vez implantada, se debe realizar una prueba de esfuerzo monitorizando las conexiones simultáneas y analizando el comportamiento del sistema. Para tal fin, una prueba controlada con la ayuda de los usuarios sería el método de prueba más fiable e ideal. En caso de que esto no sea posible, el departamento de TI debería simular una prueba de carga.

b) Accesibilidad a las aplicaciones y sistemas de la organización

Las aplicaciones web y los sistemas que funcionan con protocolos de acceso a Internet estándar (por ejemplo, http, https), así como las interfaces de usuario ligeras (por ejemplo, html, JavaScript) deben ser accesibles de manera inmediata después de establecer la conexión VPN.

Las aplicaciones y sistemas que implican interfaces de usuario pesadas o protocolos no estándar pueden no ofrecer la experiencia de usuario requerida. Es posible que no ofrezcan tiempos de respuesta aceptables o que ni siquiera funcionen. Por esto, se debe testar el acceso remoto a este tipo de aplicaciones. Si no se puede acceder a ellas de forma eficiente a través de una VPN, debería considerarse una solución de tipo VDI (Virtual Desktop Infrastructure).

Si el usuario ya dispone de un ordenador en su lugar de trabajo, una solución rápida que no requiere la implantación de una VDI es que el usuario se conecte remotamente abriendo primero una conexión VPN y luego una conexión RDP (Remote Desktop Protocol) contra el PC de la oficina. Microsoft Windows dispone de una aplicación llamada "Conexión a escritorio remoto" que permite establecer una conexión entre ordenadores Windows. Se trata de una solución rápida y sencilla recomendada en los casos en los que el usuario en modo remoto se tenga que conectar a un ordenador físico situado en las inmediaciones de la organización. En este caso, hay que tener en cuenta ciertas condiciones tales como:

UN Copyright © 2022

- Dependiendo de la configuración elegida, podría ser necesario asegurarse de que algunos equipos informáticos situados en las inmediaciones del puerto (por ejemplo, servidores, PC) se mantengan operativos ("encendidos") para que el acceso remoto sea factible.
- Habilitar la funcionalidad WOL (Wake On Lan) para que en caso de necesidad (tras un apago involuntario o un corte de luz) puedan ser encendidos a distancia por el departamento de informática.
- El ordenador remoto es un ordenador corporativo que cuenta con una solución de seguridad incorporada.
- La política de acceso a la VPN debe limitar a los usuarios remotos a establecer únicamente una conexión RDP contra su propio equipo de oficina.

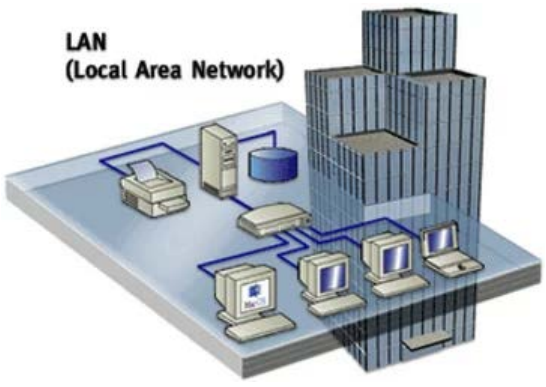
No es aconsejable instalar ninguna solución o aplicación corporativa en equipos personales o no corporativos. En su lugar, este equipo sólo debe utilizarse para establecer una conexión remota RDP con el equipo físico corporativo perfectamente reforzado o con un escritorio virtual (en el caso de tener una Infraestructura de Escritorio Virtual desplegada).

En los casos en los que sea necesario instalar aplicaciones corporativas en equipos que no sean propiedad de la empresa, se recomienda implementar una solución del tipo NAC (Network Access Control) que permita controlar los dispositivos, garantizando que cumplen con las medidas de seguridad de la organización antes de establecer la conexión remota.

Resumiendo, esta sección: todos los ordenadores remotos deberían tener un modo de acceso cliente o VPN, y aquellos que necesiten acceder al escritorio remoto (ya sea el ordenador físico de la oficina o un escritorio virtual) deberían disponer de un cliente de escritorio remoto.

No menos importante es el hecho de que hay que preparar un breve manual de usuario en el que se detalle cómo instalar, conectar y desconectar tanto la VPN como el Escritorio Remoto, en su caso. A menudo, las organizaciones tienden a centrarse en los medios tecnológicos y se olvidan de los usuarios que van a utilizarlos. Por ello, es importante proporcionar a los usuarios instrucciones claras y sencillas.

- Las líneas de comunicación tienen el ancho de banda necesario y suficiente para soportar el trabajo a distancia



Las líneas de comunicación – en particular el ancho de banda de la conexión a Internet – se diseñan en función de las necesidades de la organización en una situación normal. En este caso, la conexión entre los sistemas de información corporativos y los usuarios se establece principalmente a través de la LAN. La capacidad de la línea de acceso a Internet está diseñada para que puedan acceder a ella fuentes externas a la organización (por ejemplo, servicios en la nube, comunicación con terceros y acceso a servicios de Internet).

UN Copyright © 2022

En una situación de pandemia, el escenario se invierte. Los usuarios remotos utilizan su propia conexión a Internet de banda ancha WIFI o 4G/5G para acceder a recursos externos a la organización (por ejemplo, servicios en la nube, comunicación con terceros y acceso a servicios de Internet), consumiendo un ancho de banda de la línea de acceso a Internet corporativa cuando acceden a los sistemas de información internos de la organización.

Por lo tanto, es necesario asegurarse de que la línea de comunicación con Internet es suficiente como para soportar el trabajo a distancia.

Como se ha mencionado anteriormente, el acceso remoto a los sistemas y aplicaciones debe ser ágil y proporcionar una experiencia de usuario lo más parecida posible a la que se ofrece en una situación normal. Aunque siempre se utilizarán protocolos de acceso ligeros tras establecer la conexión VPN (por ejemplo, http o https para el acceso a las aplicaciones web y RDP para el resto de sistemas y aplicaciones), es necesario comprobar que la línea de conexión a Internet de la organización es capaz de soportar el tráfico entrante que supone trabajar en remoto. Para cumplir este objetivo, se recomienda realizar una prueba controlada monitorizando el ancho de banda y realizando mediciones tras abrir múltiples conexiones RDP y VPN contra las aplicaciones web de la organización. Tras realizar estas mediciones y estimar el número de conexiones RDP y VPN concurrentes, se puede realizar un cálculo aproximado del ancho de banda necesario.

No menos importante es la necesidad de dar instrucciones claras y sencillas a los miembros de la organización para evitar que la línea de internet corporativa se colapse, indicando que:

- La conexión VPN sólo debe utilizarse para acceder a los servicios internos de la organización, a las aplicaciones web corporativas y a una conexión de escritorio remoto.
- No debe establecerse ninguna conexión VPN para acceder a servicios en la nube, comunicarse con terceros o acceder a servicios de Internet.

A lo largo de esta sección, se ha hecho hincapié en la importancia de proporcionar instrucciones claras y sencillas sobre cómo proceder en el caso de los empleados que teletrabajan. Se recomienda que estas instrucciones vayan acompañadas de un pequeño seminario web o de formación. Una opción es grabar un vídeo formativo y subirlo a la intranet de la organización.

3.2 Herramientas de productividad en el teletrabajo

En una situación normal, la proximidad de los empleados y la posibilidad de desplazarse a otro lugar o ciudad si es necesario han llevado a las organizaciones a dar por sentado que las reuniones de trabajo se tienen que realizar en modo presencial.

Por ello, a la hora de establecer relaciones comerciales (tanto internas como externas), pocas organizaciones han visto la necesidad de implantar soluciones de teletrabajo (como las videoconferencias, chat, trabajo en la nube, redes sociales corporativas, etc.) porque, bajo el supuesto de presencia in situ, el retorno de la inversión (ROI) puede ser bajo.

UN Copyright © 2022

En una situación de pandemia, las herramientas que permiten a los compañeros de trabajo interactuar entre sí a distancia son necesarias, ya que eliminan la barrera de la distancia. Estas herramientas deben ser fáciles de usar y deben ofrecer una experiencia de usuario que se parezca lo máximo posible al contacto personal.

Son muchas las herramientas disponibles en el mercado que pueden ayudar al teletrabajo. Hay herramientas especializadas en videoconferencia y otras que tienen esta funcionalidad pero que además incorporan otras funciones como el chat individual, el chat corporativo, el trabajo en grupo, el intercambio de documentos y la integración de aplicaciones. Estas últimas son denominadas **plataformas colaborativas**.

Para poder hacer frente a una situación de teletrabajo, es aconsejable implantar una solución colaborativa. Dependiendo si la solución elegida tiene capacidad de comunicación a través de videoconferencias o no, así como de las necesidades de la organización al respecto, puede ser necesario complementarla con una herramienta de videoconferencia especializada.

En cualquier caso, las herramientas que se implementen deben ser multidispositivo de modo que deben funcionar independientemente del dispositivo que tenga el teletrabajador (ya sea un smartphone, tableta, ordenador portátil o de sobremesa, entre otros).

Ejemplos de plataformas colaborativas son Google Workspace y Microsoft 365, y ejemplos de herramientas especializadas para videoconferencias son Zoom, Microsoft Teams y Cisco Webex.

Las **principales funcionalidades básicas** que se deben proporcionar estas herramientas a los empleados en modo remoto son:

- **El correo electrónico**: El correo electrónico es la herramienta por excelencia en la comunicación digital a distancia. Las organizaciones suelen tener ya un sistema o servicio de correo electrónico, pero deben asegurarse de que este servicio se haya desplegado en todos los departamentos y de que cada empleado tenga una cuenta de correo electrónico.
- **Videoconferencia**: Una herramienta de videoconferencia sustituye a las reuniones presenciales y debe permitir una interacción ágil y eficiente entre los asistentes a las reuniones, proporcionando funcionalidades básicas como compartir la pantalla y moderar la reunión. Es importante tener en cuenta que tanto las personas de la propia organización como las ajenas a ella deben poder asistir a las reuniones celebradas por videoconferencia. Por lo tanto, la organización debe seleccionar una herramienta que permita a los participantes poder unirse y participar en las reuniones virtuales independientemente del hardware y software que tengan instalado en su dispositivo.
- **Llamadas de audio**: La mayoría de las plataformas permiten, a través de la misma herramienta de videoconferencia, realizar llamadas de audio a otros usuarios de la plataforma mediante VoIP (voice over internet protocol). Las llamadas a terceros (ajenos a la plataforma) y que requieren conexión al sistema telefónico suelen tener un coste adicional y pueden requerir una pasarela de integración con el sistema telefónico corporativo.

UN Copyright © 2022

- **Mensajería instantánea**: Esta función permite a los usuarios enviar un mensaje "emergente" a una persona concreta, a un grupo de personas o incluso a toda la organización.
- **Chat/canales**: Esta función permite a los usuarios establecer hilos de conversación específicos pudiendo de este modo evitar los correos electrónicos innecesarios y, en algunos casos, inmanejables.
- **Compartir documentos**: Esta función permite a los usuarios almacenar, compartir y acceder a los documentos. Algunos sistemas colaborativos tienen la capacidad de coautoría que permite a los usuarios trabajar en un mismo archivo al mismo tiempo mediante la sincronización automática e instantánea de los cambios, y permitiendo también que se pueda hacer un seguimiento del historial de versiones y cambios al respecto.
- **Espacios virtuales de trabajo en grupo**: Esta función permite a los usuarios organizar a los teletrabajadores por equipos de trabajo, proyectos, departamentos, etc., de forma que sea más fácil interactuar con un determinado grupo de personas predefinido (por ejemplo, compartir documentación, chatear, enviar un mensaje instantáneo, realizar una videoconferencia o una audioconferencia, etc.).

Las organizaciones deben aspirar a implementar una solución que proporcione estas siete funcionalidades para facilitar el teletrabajo. Algunas plataformas colaborativas pueden proporcionar funciones adicionales que pueden complementar estas básicas para lograr una mayor eficiencia y agilidad en el trabajo colaborativo.

Además de implementar estas herramientas de software, es importante no olvidar las herramientas de hardware necesarias para ejecutar la solución elegida.

La dotación de dispositivos móviles, como smartphones o tabletas al personal de dirección es muy recomendable, ya que, se ha comprobado que la principal interfaz de usuario utilizada a ese nivel son los dispositivos móviles. Esto añadiría agilidad e inmediatez a las comunicaciones.

Formación y grupo de apoyo en línea

Por último, no menos importante que la selección y el despliegue de las herramientas necesarias para el teletrabajo es la planificación de la formación y la preparación de los teletrabajadores en su uso, así como la puesta en marcha de un grupo de apoyo en línea para atender las consultas o posibles incidencias al respecto.

En función del tiempo disponible para implantar el cambio de modo de trabajo (del modo presencial al remoto), habrá diferentes **alternativas para formar a los teletrabajadores,** como, por ejemplo:

- Cursos de formación estándar;
- Sesión de formación comprimida;
- Formación específica en las materias más relevantes; y
- Emisión de instrucciones técnicas necesarias para su aplicación urgente.

Dado que los usuarios van a cambiar su entorno de trabajo y sus herramientas, es casi seguro que el número de consultas e incidencias derivadas del teletrabajo será elevado al principio. Por ello, se recomienda poner en marcha un **Grupo de Apoyo Online** para los empleados que teletrabajan.

UN Copyright © 2022

- En la medida de lo posible, el grupo de apoyo en línea debe ser un grupo dedicado y especializado para este tipo de incidencias, e independiente del grupo que se ocupa de las incidencias habituales con los sistemas de la organización. Este último debe seguir la ruta habitual definida por la organización.
- Debe haber dos canales separados: 1) para incidencias, y 2) para asuntos no urgentes como dudas o consultas. Esto permite al grupo de soporte priorizar los problemas que impiden a los empleados comenzar o continuar con el teletrabajo sobre las dudas o consultas menos urgentes relativas a cómo utilizar las herramientas recién implementadas.
- En caso de que sea necesario, se debe disponer de herramientas que permitan el acceso remoto y el control del ordenador de los teletrabajadores por parte del equipo de soporte.
- También debe haber soluciones disponibles en caso de que un problema que no pueda resolverse a distancia. Por ejemplo, si hay un problema de hardware en el portátil de un teletrabajador, se puede enviar un ordenador de sustitución a través de un servicio de mensajería, recogiendo al mismo tiempo el ordenador defectuoso para para repararlo.

En otras palabras, es necesario dotar al personal de equipos informáticos, así como de herramientas de software de colaboración para facilitar el teletrabajo. También es importante formar a todos los teletrabajadores en el uso de estos recursos.

3.3 Dejando de utilizar el papel

Los flujos de información en un entorno portuario suelen ser muy complejos e implican a un gran número de agentes. Cada movimiento de contenedores requiere múltiples comunicaciones entre los miembros de la comunidad portuaria, creando así una compleja red de información. Por ello, es necesario contar con un sistema o plataforma electrónica neutral y abierta que permita un intercambio inteligente y seguro de información entre los agentes públicos y privados. Con este objetivo se crearon los **Port Community Systems** (PCS).

Los PCS tienen como objetivo optimizar, gestionar y automatizar los procesos portuarios y logísticos de forma eficiente a través de una única transmisión de datos y la conexión con las cadenas de transporte y logística, con el fin de lograr:

- Mayor eficiencia en las transacciones
- Optimización de recursos
- Automatización de procesos
- Ahorro de costes
- Menos errores
- Ahorro de tiempo
- Mejor servicio al cliente

UN Copyright © 2022

Además del PCS, los agentes u organizaciones que han optado por digitalizar sus procesos están apostando por una cultura sin papel. Hay muchas razones para pasar a los medios digitales y fomentar la reducción del uso del papel en la organización. Algunas de las ventajas de una cultura sin papel son:

- √ **Seguridad, protección y fiabilidad**. El almacenamiento en formato digital nos permite controlar toda la información y saber quién y cuándo accede a los documentos.
- √ **Mayor productividad**. La gestión electrónica de documentos agiliza los procesos de consulta y gestión de la información.
- √ **Optimización de recursos**. El almacenamiento digital elimina los costes del proceso tradicional derivados, por ejemplo, de la impresión, el envío por correo y la destrucción de papel.
- √ **Mejora del medio ambiente.**
- √ **Firma electrónica**. Podemos firmar documentos electrónicamente desde cualquier lugar y dispositivo móvil, reduciendo el tiempo necesario para cerrar acuerdos, negociaciones, etc.

Afortunadamente, las plataformas de PCS permiten la digitalización de los principales procesos de la cadena logística. El primer paso es determinar si ya existe una cultura sin papel totalmente implantada. En tiempos de pandemia, en los que el personal trabaja a distancia, los procesos que aún se gestionan en papel son un hándicap de modo que hay que esforzarse por digitalizarlos.

Por lo tanto, es necesario identificar los procesos que aún no están digitalizados y abordarlos caso por caso. En función del tiempo disponible para llevar a cabo su digitalización, ésta podrá realizarse con un mayor o menor grado de automatización.

Existen herramientas gratuitas que pueden ayudar a la hora de deshacerse de los procesos en formato papel. Los pasos para un proceso sencillo con poca automatización podrían ser:

1. **Creación**: Utiliza el procesador de textos (por ejemplo, Microsoft Word o Google Docs) de la plataforma colaborativa para digitalizar/convertir a formato estándar PDF (Portable Document Format) cualquier documento generado en la organización.
2. **Firma**: Si el documento requiere una firma, se puede utilizar el portafirmas electrónico corporativo o la aplicación Adobe Acrobat Reader DC.
3. **Distribución**: Utiliza las herramientas de gestión del correo electrónico (por ejemplo, Microsoft Outlook o Google Gmail) o de compartición de documentos (por ejemplo, Microsoft OneDrive/SharePoint o Google Drive) disponibles en la plataforma colaborativa.

Estas herramientas y pasos deben formar parte de la fase de comunicación y formación mencionada en el apartado anterior.

En resumen, hay que identificar los procesos que aún se mantienen en formato papel para ayudar a centrar los esfuerzos de digitalización. Se recomienda que la transición hacia la eliminación del papel se aborde de forma gradual. Inicialmente, maximizar el proceso de la automatización no debería ser una prioridad debido al tiempo necesario para ello. Esto podría abordarse en una fase posterior.

UN Copyright © 2022

3.4 Seguridad y resiliencia informática

En una situación normal, los recursos informáticos de la empresa están conectados y son accesibles a través de la LAN de la organización. La mayoría de las aplicaciones, bases de datos, equipos (PC), etc. están interconectados a través de una red fiable y segura. En esta situación, uno de los pilares más importantes de la seguridad informática es la seguridad perimetral, es decir, se establece un perímetro de seguridad alrededor de la red de la organización. La práctica habitual es proteger el perímetro de la LAN con dispositivos de tipo cortafuegos, que permiten el acceso seguro de los ordenadores de la red a los recursos del exterior evitando de este modo que los ordenadores del exterior accedan a los recursos y sistemas internos de la empresa.

Sin embargo, en una situación de teletrabajo, los equipos de los teletrabajadores (por ejemplo, los PC) deben salir del perímetro de seguridad establecido en una situación normal y, a efectos del sistema de seguridad perimetral de la organización, serán tratados como cualquier otro equipo conectado a Internet, es decir, como equipos no fiables.

Cuando los empleados trabajan a distancia es más difícil controlar y detener las amenazas. En esta situación, surgen nuevos riesgos (ciberriesgos) que deben ser evaluados, tratados y mitigados en la medida de lo posible.

A continuación, se detallan las recomendaciones y acciones que debemos tener en cuenta para conseguir un entorno informático lo más seguro posible y, reconociendo que no es posible garantizar una seguridad absoluta, se deben disponer de medidas de recuperación rápida para responder en caso de sucedan ataques deliberados. Las acciones en cuestión son:

Recomendaciones generales

Como medidas generales de protección, se recomienda:

- √ Tener instaladas las últimas actualizaciones del sistema operativo;
- √ Implementar un protocolo de autenticación fuerte y un Directorio Activo de la organización. En el caso de los servicios en la nube o el acceso a la VPN, se recomienda no tener solo acceso con contraseña, sino contar con un sistema de autenticación de dos factores (2FA);
- √ Proteger el BIOS (Sistema Básico de Entrada/Salida) con una contraseña fuerte;
- √ Disponer de soluciones de seguridad específicas en los puestos de trabajo: complementar el tradicional y necesario antivirus (EPP - Endpoint Protection Platform) con una solución de tipo EDR (EndPoint Detection and Response);
- √ Implantar una política de administración de los equipos de trabajo centralizada, donde los usuarios no tengan credenciales de administrador;

UN Copyright © 2022

- √ Proteger la información. La mayoría de los portátiles profesionales cuentan con un chip TPM (Trusted Platform Module) mediante el cual se pueden cifrar los datos del disco duro, protegiendo la información incluso en caso de acceso físico al disco;
- √ Tener una lista actualizada de personas, direcciones IP, teléfonos, correos electrónicos del personal que accede a los sistemas de forma remota;
- √ Revisar los registros y auditar las conexiones remotas;
- √ Restringir el montaje de unidades de organización mapeadas en ordenadores remotos que no sean seguros.

Diagnosticar nuevas amenazas

El teletrabajo conlleva varios riesgos que hay que tener en cuenta de antemano para aplicar soluciones más seguras.

El inicio de una crisis como una pandemia trae consigo la necesidad de información. La gente necesita saber qué hacer en caso de contagio, qué medidas de protección hay que tomar, cómo evoluciona la pandemia, qué previsión de vacuna hay, etc. Sin embargo, este hecho es aprovechado por los ciberdelincuentes.

A modo de ejemplo, se han registrado más de 20.000 dominios que utilizan términos relacionados con COVID-19, de los cuales más del 50% de los registros se hicieron en marzo de 2020 (mientras algunas partes del mundo se encontraban completamente encerradas) muchos de ellos con fines claramente maliciosos. Por esto, se necesitan soluciones de prevención y tecnología para hacer frente a estas nuevas amenazas.

Prevenir

Los correos electrónicos son un punto de entrada para los ataques de phishing. En periodos de pandemia, abundan los correos electrónicos con asuntos y direcciones de mensajes que parecen ser fuentes oficiales y fiables que tratan el tema de la pandemia. Sin embargo, detrás de estos mensajes hay archivos o enlaces altamente peligrosos.

Es importante informar adecuadamente a los empleados de la existencia de este peligro, ya que pueden desconocer esta realidad.

UN Copyright © 2022

Formar

La organización debe instruir a sus trabajadores sobre cómo proteger sus equipos y conexiones informáticas cuando trabajen a distancia, así como verificar que se estén utilizando técnicas adecuadas de encriptación de equipos y sistemas de autenticación seguros. Además, los empleados deben recibir formación sobre cómo hacer frente a una amenaza o ciber-ataque de acuerdo con el protocolo de la organización. En este sentido, se recomienda realizar una campaña de phishing simulada que ayude a los empleados a entender el problema de forma tangible, entrenándolos para situaciones reales.

Plan de contingencia

Las organizaciones mejor preparadas cuentan con un plan de contingencia que les permite anticiparse a las dificultades que puedan surgir. Por el contrario, las que se han visto sorprendidas por la situación sin un plan de actuación o incluso se han visto obligadas a improvisar un sistema de teletrabajo por la falta de planificación, han visto colapsar sus sistemas por el aumento en el tráfico de acceso remoto y han tenido que dotar a los equipos remotos de medidas de seguridad de manera precipitada.

Está claro que ninguna empresa quiere detener su actividad. Para evitarlo, hay que diseñar un **Plan de Contingencia Empresarial** y ponerlo a disposición de los trabajadores implicados. Este plan debe probarse periódicamente para confirmar su validez y eficacia, y actualizarse en caso de ser necesario. Tener un Plan de Contingencia no probado u obsoleto es inútil.

Ciber-resiliencia

Hoy en día, las organizaciones dependen de la tecnología para desarrollar y mantener su actividad. En la era de la transformación digital, una brecha de seguridad puede paralizar los negocios y los procesos productivos, provocando pérdidas económicas y otras consecuencias que pueden llegar a poner en entredicho la continuidad de la organización.

UN Copyright © 2022

La ciber-resiliencia es la capacidad de una organización para anticiparse, resistir, recuperarse y evolucionar para mejorar sus capacidades ante condiciones adversas, tensiones o ataques a los recursos cibernéticos que necesita para funcionar.

Decimos que una organización es ciber-resiliente si es consciente de que la seguridad absoluta no existe y, por lo tanto, asume que algunos ataques no podrán ser detenidos. Bajo esta premisa, dispone de un plan de acción que le permite reanudar la actividad de la organización lo antes posible si se produce dicho ataque.

La organización que cuente con planes de contingencia, continuidad y crisis podrá superar un ciberataque en menos tiempo y con un menor coste económico. La planificación y la prevención son las mejores formas de garantizar una adecuada protección contra los ciberataques y poder convertirse en una organización ciber-resiliente.

Medición de la ciber-resiliencia

Pero, ¿cuál es la ciber-resiliencia de mi organización? ¿Cuál es su nivel de ciber-resiliencia? En este sentido, solo se puede mejorar si se puede medir.

Para tal fin, existen métodos que permiten medir el grado de ciber-resiliencia de una organización. El marco de referencia de indicadores de ciber-resiliencia propuesto por MITRE[1] es uno de los más extendidos. Este marco se basa en los cuatro objetivos que se deben alcanzar: Anticipar, Resistir, Recuperar y Evolucionar:

- √ **Anticiparse**: estar preparado e informado para evitar que las funciones de la misión/negocio se vean comprometidas por los ataques.
- √ **Resistir**: continuar con las funciones esenciales de la misión/negocio a pesar de que de un ataque por parte de un adversario.
- √ **Recuperar**: restaurar las funciones de la misión/negocio en la mayor medida posible tras la correcta ejecución de un ataque por parte de un adversario.
- √ **Evolucionar**: cambiar las misiones/funciones empresariales y/o las capacidades cibernéticas de apoyo, con el fin de minimizar los impactos adversos de los ataques reales o previstos por el adversario.

Para lograr estos cuatro objetivos y, en última instancia, ser considerada una organización ciber-resiliente, se deben tener en cuenta los siguientes elementos:

- √ Anticiparse
  - Política de Ciberseguridad: contar con una política que establezca los requisitos para disponer de ciber-resiliencia, abordar los riesgos de ciberseguridad, asignar responsabilidades y comunicar a toda la organización.
  - Gestión de Riesgos: identificar, analizar y mitigar los riesgos para los activos de la organización, que podrían afectar negativamente al funcionamiento y la prestación de servicios.
  - Formación en Ciberseguridad: promover el desarrollo de conocimientos y habilidades de los individuos en apoyo de sus funciones, logrando y manteniendo la ciber-resiliencia y protección operativa.

1 MITRE (2012), Cyber Resiliency Engineering Framework.
https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

UN Copyright © 2022

√ Resistir

- Gestión de la vulnerabilidad: identificar, analizar y gestionar las vulnerabilidades de los recursos que dan soporte a los servicios esenciales.
- Supervisión continua: reunir, recopilar y distribuir información sobre el comportamiento y las actividades de los sistemas y las personas para apoyar el proceso continuo de identificación y análisis de los riesgos para los activos y los servicios esenciales de la organización que puedan afectar negativamente a su funcionamiento y prestación.

√ Recuperar

- Gestión de incidentes: establecer procesos para identificar y analizar acontecimientos, detectar incidentes y determinar y aplicar una respuesta organizativa adecuada.
- Gestión de la continuidad del servicio: determinar cómo la organización lleva a cabo la planificación empresarial para garantizar la continuidad de los servicios esenciales en caso de incidente o desastre. Se debe prestar especial atención al objetivo de recuperación, por lo que se cuenta con un sistema de copia de seguridad y restauración (backup o site recovery) que garantiza la existencia de copias de toda la información de la organización.

√ Evolucionar

- Gestión de la configuración y de los cambios: establecer procesos para mantener la integridad de todos los activos, tales como la tecnología, la información y las instalaciones, necesarios para prestar servicios esenciales.
- Comunicación: establecer procedimientos para garantizar la comunicación entre los responsables del funcionamiento de los servicios esenciales, tanto internos como externos a la organización.

Para resumir este apartado, ante una situación de pandemia surgen nuevos riesgos (ciberriesgos) que deben ser evaluados, tratados y mitigados. Para ello, hay una serie de recomendaciones para conseguir un entorno informático lo más seguro posible.

Teniendo en cuenta que existen riesgos y amenazas que no pueden evitarse, las organizaciones deben de ser capaces de medir su estado de ciber-resiliencia para poder avanzar en aquellos objetivos que aún no se han alcanzado y permitir la consecución de un grado de ciber-resiliencia aceptable y adecuado.

El marco estable por MITRE puede servir de referencia para medir el estado y mejorar el grado de ciber-resiliencia de una organización. Este marco se basa en cuatro objetivos (anticipar, resistir, recuperar y evolucionar), al mismo tiempo que incluye una serie de dominios funcionales en los que las organizaciones deben trabajar.

UN Copyright © 2022