Seguridad Informática en la transformación del Trabajo Presencial al Teletrabajo

Luciana Gervasoni
lucigervasoni.lg@gmail.com

Diplomatura en Seguridad Informática en Entornos Virtuales de Trabajo,
Facultad de Ingeniería, UCASAL

Resumen

Este trabajo muestra la resolución de una situación problemática que enfrenta una organización al tener que modificar su modalidad de trabajo presencial a modalidad de teletrabajo en tiempos de emergencia, apresurada por la pandemia mundial surgida a raíz del virus COVID-19.
En primer lugar, se tomaron decisiones teniendo en cuenta los recursos que se tenían al momento de la migración a la nueva forma de trabajo y, a partir de allí, se realizó un plan de seguridad que permite la integración gradual de políticas y recursos que refuerzan la seguridad de la información de la empresa.
Este programa de protección de activos de la organización contempla distintos vectores que se deben tener en cuenta para abarcar una solución sólida, incluyendo tareas continuas, mantenimiento del plan y concientización de los empleados, factores fundamentales para el éxito del procedimiento.

Palabras Clave

Seguridad teletrabajo, Políticas de seguridad, Evaluación de riesgos.

Abstract

This project shows a resolution of a problematic situation with which an organization deals by having to modify its face-to-face work modality to work from home in emergency times, rushed by the world pandemic arising from COVID-19 virus.
In first place, some decisions were taken considering the resources that the organization had at the moment of the migration and, starting from there, a security plan was made allowing the integration of policies and resources that reinforce the company information security.
This program of organization asset protection includes different vectors that must be taken into account to cover a solid solution, including continuous tasks, plan maintenance and employee training, fundamental factors for the success of the procedure.

Keywords:

Security in homework, Security policies, Risk assessment.

Introducción

En el presente trabajo se plantea una situación empresarial actual en la que una organización decide comenzar a trabajar con algunos de sus empleados fuera de la institución. Esta nueva modalidad de trabajo, llamada teletrabajo o home-office, es adoptada por aquellos empleados que realizan sus tareas diarias desde su casa.

La organización pone a disposición sus recursos humanos, materiales y financieros para lograr esta migración de la mejor manera y como principal objetivo mantener la seguridad, integridad y confidencialidad de los activos de la empresa.

El Departamento de Seguridad informática se hace cargo de las políticas de seguridad y del programa de seguridad que se presenta a la Gerencia de la empresa para su aprobación y puesta en marcha.

2. Situación de la empresa

Una obra social de la ciudad de Santa Fe tiene alrededor de 300 empleados y, en su cartilla médica, más de 1000 prestadores de servicios de la salud (médicos de distintas especialidades, kinesiólogos, oculistas, etc.). La cantidad de socios es de alrededor de 15000.

Al inicio del aislamiento social obligatorio, la empresa tuvo que adaptarse a las circunstancias y seguir operando de igual manera (dentro de lo posible). Parte de sus empleados continuaron trabajando en sus puestos de trabajo físico y otros tantos comenzaron a trabajar desde sus casas con los elementos que tenían.

Hoy en día, la obra social desea implementar el teletrabajo para los empleados de los sectores de Atención telefónica, Sistemas, Ventas y Socios, siendo un total de 150 trabajadores aproximadamente.

Sus tareas serán, según cada sector:

- Atención telefónica: recibir las llamadas de socios, atender sus inquietudes y despejar sus dudas. Transferir llamadas al sector correspondiente.
- Sistemas: encargados de la infraestructura y redes, desarrollo de la aplicación de la obra social, y seguridad de la información.
- Ventas: encargados de contactar nuevos posibles socios y vender los planes de salud.
- Socios: encargados del alta, baja, y modificación de datos de socios.

La empresa dotará de computadoras portátiles y teléfonos celulares a todos los empleados en modalidad de teletrabajo. Además, proveerá de escritorios y sillas a quienes lo soliciten. El presupuesto para esta operación y para fortalecer la infraestructura actual de la empresa es de U$S200.000.

3. Seguridad Informática

En los siguientes apartados se define la organización y estructura de la seguridad informática, considerando particularmente todo lo relativo a la política de seguridad que será necesario implementar, así como el programa de seguridad pertinente.

3.1. Política de Seguridad

Se define en términos de los objetivos, alcance, comunicación, propietarios de las políticas y normas, que se describen detalladamente a seguir:

Objetivos:

- Desarrollar la estrategia necesaria para cuidar de los activos de la información de la organización al momento de tener a sus recursos humanos trabajando desde sus hogares.
- Mantener los estándares de seguridad de la información que se encuentra tanto dentro como fuera de la empresa respondiendo a su integridad, confidencialidad, no repudio y autorización de acceso.

Alcance:

Esta política establece normativas para alcanzar y mantener la seguridad de la información de la empresa al momento de tener a sus empleados trabajando en sus casas.

Comunicación:

La política de seguridad para el teletrabajo será comunicada a la totalidad de empleados,

luego de ser aprobada por la alta gerencia y presentada por el Departamento de Seguridad de la Información. Este departamento será el encargado, no sólo de comunicar la política, sino de capacitar a los distintos recursos humanos para su completo entendimiento.

Propietarios de las políticas:
El Departamento de Seguridad de la Información será el encargado de controlar si esta política es cumplida por todos los empleados. En caso de haber algún incumplimiento, se informará al jefe del departamento y se ejecutarán las acciones necesarias para corregir esta situación.

Normas:
Las normas abarcan los siguientes espacios: escritorios de trabajo, Conectividad, Políticas de contraseñas y Permisos de usuarios, y se definen en detalle a continuación:

a. Escritorio de trabajo:
- Cada empleado utilizará diariamente la notebook brindada por la empresa.
- Se entregará la misma con Windows 10 instalado. Se deben aceptar e instalar todas las actualizaciones que proponga el sistema operativo.
- La notebook tendrá instalado el sistema Antivirus de Kaspersky, controlado por el servidor Kaspersky Security Center instalado en la infraestructura de la empresa.
- Se podrá instalar software legal solamente necesario para actividades laborales y se debe mantener actualizado.
- Evitar descargar archivos y programas que no sean de páginas oficiales.
- Utilizar política de bloqueo de pantalla: la pantalla se bloqueará luego de 10 minutos de no haberse movido el cursor.
- Estará prohibido conectar dispositivos USB o discos externos a las notebooks. En caso de necesitar hacerlo exclusivamente por trabajo, se dará un permiso temporal.

b. Conectividad:
- La notebook puede conectarse por Ethernet o WiFi, siempre a redes privadas y seguras. No se permite conectarse a redes públicas.
- La conexión a la empresa será a través de la VPN que se puso a disposición. Cada empleado ingresará con su usuario y contraseña de Active Directory (Microsoft). Se utilizará un factor de doble autenticación: será un código enviado al celular empresarial del empleado, que luego escribirá en la notebook para completar la conexión.
- Al ingresar la contraseña para conectarse a la VPN, el sistema admitirá hasta 9 intentos de inicio de sesión erróneos, a la décima vez se bloqueará el usuario por 20 minutos. De ocurrir una vez más el bloqueo en un lapso de tiempo corto, se deberá pedir el desbloqueo de usuario a personal de Seguridad de la Información.

c. Política de contraseñas:
- Se solicitarán contraseñas robustas. Su longitud mínima será de 9 caracteres y deben poseer al menos una letra mayúscula, una minúscula, un símbolo y un número.
- Se deben cambiar las contraseñas cada dos meses.

d. Permisos de usuarios:
- Cada usuario en la VPN tendrá permisos para conectarse solamente a su escritorio remoto en la empresa. Desde este, se podrá mover dentro de la red, según corresponda y con los permisos que siempre tuvo.

3.2. Programa de seguridad
Este programa ofrece una forma de alcanzar las metas y objetivos de la organización, relacionados con la seguridad de la información, y se describe según las instancias de trabajo siguientes:

Evaluación de riesgos:
En el primer paso del programa de seguridad se deben identificar los riesgos a los que está expuesta nuestra organización al tener trabajando empleados en sus casas. A partir de esto, la información no sólo está almacenada en el interior de la empresa, sino que también está disponible en donde se encuentre cada una de

las notebooks y celulares distribuidos.

Para la evaluación de riesgos, primero se deben identificar los activos [1]: firewall, escritorios físicos en empresa, notebooks en home-office, celulares, empleados, información. En segundo lugar, se deben identificar las amenazas y vulnerabilidades a los que cada uno de estos activos está expuesto:

a. Firewall: puede ser atacado por hackers que intenten ingresar a la infraestructura de la empresa. Tipos de ataques: DoS, ataque de fuerza bruta.
b. Escritorios físicos en la empresa: al tener el protocolo RDP habilitado para la conexión de empleados en home-office, queda expuesto el puerto correspondiente y es más sencillo ingresar al mismo remotamente. También podría sufrir ataques de fuerza bruta si alguien quisiera ingresar como usuario.
c. Notebooks en home-office: si la red a la que se conectan no es segura, se corre el riesgo que accedan atacantes a la notebook y roben información. Además, si la notebook queda desbloqueada en algún momento, cualquier integrante de la casa podría acceder a la misma.
d. Celulares: la amenaza más grande se corre en el caso de pérdida o robo del celular. Éste debe tener bloqueo de pantalla (en lo posible biométrico) y de tarjeta SIM. También podría ser víctima de algún virus a través de la descarga de archivos.
e. Empleados: es el eslabón más débil de la cadena. Los empleados pueden ser engañados a través de métodos de ingeniería social y descargar distintos tipos de malware o entregar contraseñas sin saberlo [2].
f. Información: puede ser robada a través de los distintos métodos mencionados y más. Hay riesgo de que sea robada, de que se borre o que se divulgue.

El siguiente paso es calcular el nivel de riesgo de cada uno de ellos. Esto se logra a partir de la probabilidad de ocurrencia que tiene y del impacto que pueda llegar a tener en la organización el hecho de que el riesgo ocurra.

Para nuestra organización, los niveles de riesgo son los siguientes:

Tabla 1: Escala de riesgos

Impacto	Probabilidad de ocurrencia		
	Baja	Media	Alta
Bajo	Bajo	Bajo	Medio
Medio	Medio	Medio	Alto
Alto	Alto	Alto	Alto

Estrategia para mitigar riesgos:

Mitigar un riesgo es tomar una acción para disminuir el impacto del mismo [3]. A continuación, se establecen las estrategias para mitigar los riesgos:

a. Firewall: se deben activar todos los controles de antivirus y antimalware que posee el firewall. Se debe habilitar el acceso a su configuración (GUI) sólo para un usuario administrador y éste podrá ingresar solamente estando en la red local. Se habilitará el acceso para este mismo usuario por CLI a través de SSH. Se bloquearán todos los puertos que no sean exclusivamente utilizados por alguna aplicación. Se habilitará el acceso por VPN para empleados de home-office. Las contraseñas de usuarios y accesos deben ser seguras.
b. Escritorios físicos en la empresa: todos los escritorios físicos de la empresa se encontrarán en la red protegida por el firewall. Se cierran los puertos que no son utilizados. Las contraseñas de usuarios serán seguras. Se deshabilitan los puertos USB. Se bloquean las pantallas a los 10 minutos de no haber movimiento.
c. Notebooks en home-office: la conexión a internet será a través de una red segura y privada. Las contraseñas de usuarios serán seguras. Se deshabilitan los puertos USB. Se bloquean las pantallas a los 10 minutos de no haber movimiento.
d. Celulares: deben tener bloqueo de pantalla: numérico y biométrico (dentro de lo posible), puede ser a través de huella o de iris, según lo permita el dispositivo. La tarjeta SIM debe tener un PIN de bloqueo

para ocultar los contactos. El celular debe tener el antivirus de Kaspersky con el que se entrega.

e. Empleados: se capacitarán los empleados en cuanto a Seguridad Informática para que sepan responder a posibles ataques o evitar los mismos en caso de tener la posibilidad. Se distribuirá información periódicamente para reforzar los conocimientos.
f. Información: se establecerá la encriptación de la información almacenada en las notebooks y la información sensible de los celulares. Se hará backup de las notebooks: un full por semana y un incremental por día, el resto de los días.

Requerimientos de seguridad:

La empresa debe contar con la política de seguridad de la información y su respectivo programa de seguridad. Ambos deben estar aprobados por la alta gerencia de la organización. El Departamento de Seguridad debe constatar que se cumplan e informar sus estados periódicamente.

Recursos internos y externos necesarios:

La implementación del programa formulado requerirá de recursos para su desarrollo, entre los que se pueden indicar:

a. Recursos humanos encargados de llevar a cabo la gestión de la seguridad de la información: 2 analistas de seguridad y un jefe.
b. Recursos materiales: infraestructura de firewall para la conexión remota, notebooks, celulares. Licencias de Windows y antivirus Kaspersky. En algunos casos se pueden requerir elementos de escritorio: escritorio, silla.
c. Recursos financieros: para este proyecto se estimó un presupuesto aproximado de USD 200.000.

Infraestructura de seguridad y nuevas tecnologías:

La infraestructura de seguridad está compuesta principalmente por un firewall FortiGate 200E que se va a adquirir, que es el que permitirá la conexión de los 150 empleados en home-office a la infraestructura interna de la organización a través de la VPN SSL. Esta solución permite el monitoreo de conexiones, sesiones de usuarios y eventos que surjan durante cada jornada laboral.

La infraestructura de seguridad interna cuenta con un servidor anti-malware instalado en los servidores de la empresa, de la marca Kaspersky, que contará con políticas para las notebooks y celulares en home-office. Con la solución de Kaspersky, además, se podrá llevar un registro de eventos de seguridad que vayan sucediendo.

A partir de los dispositivos incorporados (notebooks y celulares) se aplicará la identificación de usuarios mediante biometría: reconocimiento de iris y de huellas digitales.

Para recuperar información perdida la empresa cuenta con la solución Veritas Backup Exec que se aplicará a notebooks y configuración del firewall.

Perímetro de seguridad:

En lo que respecta al perímetro de seguridad lógica, como se dijo anteriormente, va a estar a cargo de la solución de FortiGate. En lo que respecta a seguridad física, los equipos de la empresa se encuentran en un datacenter principal, ubicado en el interior de la empresa, cuidado de riesgos de intrusión y ambientales. Además, se cuenta con un datacenter secundario en otra ubicación y con los mismos cuidados.

Seguridad del equipamiento:

En cuanto a soluciones que se encuentran dentro de la empresa, como se aclaró anteriormente, cuentan con seguridad dentro de los datacenters. En cuanto a requerimientos de energía, cada uno de ellos contiene UPS APC para certificar su uso continuo.

Cada notebook y celular entregados a los empleados estarán anotados en un libro de registros. Si bien cuentan con seguro por robo, cada empleado deberá hacerse cargo del cuidado del equipamiento.

Políticas de seguridad y comunicación:

La empresa cuenta con una política de seguridad descripta en el apartado anterior. La comunicación de la misma y cada una de sus actualizaciones están a cargo del equipo de

Seguridad de la Información.

Documentación:
El equipo de Seguridad de la Información es el encargado de generar por primera vez la documentación de todo el plan y políticas de seguridad para el teletrabajo y mantenerla actualizada a medida que surjan distintos cambios.

Métricas:
Se crearán distintos indicadores que marquen la tolerancia máxima de eventos que pueden surgir mes a mes en lo que respecta al home-office. Cuando alguno de estos indicadores supere el límite, se revisarán los procesos nuevamente y se generará al menos un cambio que indique la supuesta mejora de la implementación. Los indicadores serán: cantidad de riesgos acontecidos (riesgos bajos, medios y altos por separado), cantidad de ataques de malware (internos y externos por separado), cantidad de equipos infectados, cantidad de daños en equipamientos por catástrofes naturales, cantidad de intentos de intrusión en la VPN, cantidad de intrusiones en la VPN, cantidad de equipos de home-office dañados por cualquier causa.

Tareas continuas:
- Concientización de los empleados: el equipo de Seguridad de la Información será el encargado de generar capacitaciones a cada uno de los empleados que comenzará a trabajar en home-office. Una vez que estén establecidos, se capacitará al resto de los empleados de la empresa.
- Monitoreo: el equipo de Seguridad Informática será el encargado de controlar los eventos almacenados en las distintas soluciones que son parte del teletrabajo y controlarán las métricas establecidas.
- Mantenimiento del programa: el equipo de Seguridad Informática será el encargado de reevaluar el programa y la política de seguridad de la empresa cada vez que los indicadores y la política de métricas así lo disponga.

4. Infraestructura de Red
En el programa de seguridad que se estableció para la empresa, en el apartado anterior, se muestran algunos riesgos de tener parte de la infraestructura fuera de la oficina. Además, se establece la importancia de cada riesgo: baja, media y alta, según su impacto y su probabilidad de ocurrencia. A partir de esto, se detallan algunas de las amenazas más importantes que tiene la infraestructura de red del negocio y su clasificación para, posteriormente, detallar su plan de mitigación:

a. Firewall: ingreso de atacantes a la VPN. Amenaza externa.
   Probabilidad de ocurrencia: media.
   Impacto: alto.
   Riesgo: alto.
   Mitigación: se deben activar todos los controles de antivirus, antimalware e IPS que posee el firewall. Se debe deshabilitar el acceso a su administración (mediante GUI y CLI) para usuarios que se encuentren fuera de la red interna y sólo para un usuario administrador. Se habilitará el acceso para este mismo usuario por CLI a través de SSH y de GUI a través de HTTPS.
   Se bloquearán todos los puertos que no sean exclusivamente utilizados por alguna aplicación. Ingreso a la VPN: se habilitará el acceso por VPN para empleados de home-office: las contraseñas de usuarios deben ser seguras, según lo estipulado en la política de seguridad presentada anteriormente. Esta última también estipula el bloqueo de usuarios luego de una cierta cantidad de intentos de ingresos erróneos.
b. Notebooks en home-office: infección de las notebooks a través de la descarga de archivos maliciosos.
   Amenaza interna.
   Probabilidad de ocurrencia: alta.
   Impacto: alto.
   Riesgo: alto.
   Mitigación: todas las notebooks tendrán el antivirus Kaspersky instalado y actualizado. Este reportará cualquier incidente al usuario y al administrador de la consola antivirus.
c. Notebooks en home-office: hackers podrían ingresar a la red de la notebook y a la información que hay en ella.

Amenaza externa.
Probabilidad de ocurrencia: media.
Impacto: alto.
Riesgo: alto.
Mitigación: en primer lugar, se concientizarán a todos los empleados que trabajen en home office sobre la importancia de la red a la que se conectan para trabajar: esta red debe ser segura y privada. Su contraseña de acceso debe ser compleja. Los discos de las notebooks poseerán encriptación para evitar que hackers se queden con información confidencial. Otra opción de mitigación es el mismo antivirus que tendrán instalado.

d. Correo electrónico: empleados pueden ser presa de correos de Phishing e ingresar a una web malintencionada las claves de usuario para acceder a la VPN y al equipo de trabajo.
Amenaza interna.
Probabilidad de ocurrencia: baja.
Impacto: alto.
Riesgo: alto.
Mitigación: concientización a los empleados que trabajen en home office y luego a todos los empleados de la empresa, sobre los ataques de ingeniería social. Se les enseñará a reconocer los distintos tipos de ataques y cómo defenderse.

5. Cloud Computing

Dentro de todos los servicios que se tienen en la red empresarial, se podría elegir la migración del servicio de backup a la nube. Como se comenta en el primer apartado (Seguridad Informática), la empresa posee la solución de backup Veritas Backup Exec [4] on-premise. Actualmente, los backups se guardan tanto en el datacenter principal, como en el secundario.

A partir de esto, se propone migrar el servicio de backup a la nube. Veritas posee en su software de backup, la posibilidad de realizar el backup en la nube, y también recuperarlo desde ahí mismo, desde donde sea que se esté ya que es administrable desde la nube también.

Recomendaciones de seguridad a tener en cuenta:

Veritas trabaja con la nube de AWS o Azure. Se debe elegir la solución indicada teniendo en cuenta las consideraciones de ambos proveedores (tanto Veritas como el que se elija):

a. Disponibilidad del servicio en la nube: el proveedor debe garantizar servicio continuo y demostrar que está preparado frente a caídas tanto en su infraestructura como de DoS provenientes de ataques informáticos. Deben tener un Plan de Contingencia adecuado en caso de que algo falle.
b. Los servidores de almacenamiento tanto de software (Veritas) como de los backups (AWS o Azure) realizados deben tener a su vez copias de backup en distintos servidores.
c. Revisar las políticas de seguridad de los proveedores y su cumplimiento.
d. Revisar que la infraestructura de los proveedores posea soluciones frente a ataques informáticos. Política de información de ataque: definir con anterioridad qué información deberá entregarse a la empresa cliente en caso de que la infraestructura de alguno de los proveedores sufra un ataque.
e. Establecer mecanismos de monitoreo y control de acceso de usuarios y tareas que se realicen en la plataforma.
f. Definir la ubicación de los servidores de los proveedores: las leyes en cuanto a protección de datos personales varían en cada país, por lo tanto, debe tenerse en cuenta que concuerden con las de Argentina.
g. Solicitar un contrato de privacidad y confidencialidad en cuanto a la información de nuestra empresa que ellos puedan tener desde la implementación del servicio en adelante y qué se realizará con ella una vez que el contrato finalice.
h. Tener en cuenta la experiencia y el conocimiento de las personas encargadas del soporte de la solución.
i. Solicitar el programa de actualizaciones de software en cuanto a parches de vulnerabilidades descubiertas.
j. Se debe tener en cuenta que exista la posibilidad de tener distintos tipos de usuarios en la plataforma de backup en la

nube, con diferentes permisos.

k. Se recomienda limitar las direcciones IP permitidas al acceso de la plataforma de backup.
l. Solicitar, en caso de tener la posibilidad, un doble factor de autenticación a la plataforma.

En cuanto a la integración de Veritas Backup Exec con el resto de la infraestructura, no habría problemas de ningún tipo ya que este proveedor soporta no solo multi-cloud sino también plataformas híbridas [5].

6. Virtualización

A continuación, se mencionan las distintas virtualizaciones que se realizarán en el proyecto para lograr que los empleados de la empresa realicen home-office:

- Virtualización de servicios: como se menciona en el apartado anterior, se virtualizará el servicio de backup de la organización para brindar un acceso seguro a los datos de la organización mediante el software Veritas Backup Exec (ver apartado 3 para más detalles).
- Virtualización de infraestructura: la virtualización más importante de toda la implementación de home-office es la de la red privada virtual (VPN) que permite la conexión de los empleados a la red interna de la empresa desde distintos puntos geográficos. De esta manera, el tráfico que se genera viaja cifrado dificultando a un tercero que pueda robar información confidencial [6].

Como se indicó anteriormente, el equipo que se adquiere para generar esta red virtual es el FortiGate 200E, que cubre y supera las necesidades para mantener la conexión de todos los empleados destinados a home-office.

6. Sistemas colaborativos

La empresa de salud publicitará sus Planes de Salud para las distintas edades y Planes Familiares tanto en Facebook como en Instagram. Además, se comunicará con los clientes o futuros socios a través de estas redes sociales y de WhatsApp. En primer lugar, se hacen recomendaciones en cuanto a las cuentas de la organización en estas aplicaciones y luego en lo que respecta a las publicaciones y envío de mensajes.

Recomendaciones a la hora de la creación de las cuentas de Facebook, Instagram y Whatsapp:

- Asociar las cuentas a un número de teléfono empresarial.
- Definir el tipo de cuenta como empresarial y realizar la verificación en caso de corresponder.
- Colocar una contraseña segura, como se explica en el apartado 1 de este proyecto (sección Seguridad Informática).
- Habilitar el doble factor de autenticación en cada una de las aplicaciones.
- Activar el monitoreo de inicio de sesión.

Se recomiendan los siguientes aspectos de seguridad en cuanto a las publicaciones:

- Subir fotos y/o videos de elaboración propia.
- No descargar cualquier tipo de archivo que pueda subir el público en general en los comentarios de las publicaciones.
- En caso de tener comentarios de cuentas extrañas, eliminarlos y bloquearlos.
- Tener instalado el antivirus Kaspersky en todos los dispositivos en los que se acceda a las redes sociales.

En lo que respecta a la comunicación con los clientes se realizan las siguientes recomendaciones de seguridad:

- Interactuar siempre con perfiles identificables.
- No entregar información confidencial ni personal a ningún usuario.
- En el caso de recibir mensajes inapropiados, denunciar el comentario y el perfil que corresponda.

7. Teletrabajo

Para esta nueva modalidad que adopta la empresa para algunos sectores de trabajadores, el modelo de teletrabajo más adecuado es el de Teletrabajador en Casa durante el período de la pandemia. Luego de finalizado el período se podría revers si pueden pasar a ser teletrabajadores flexibles.

Las características distintivas de este modelo son:

- Realización del trabajo en un lugar distinto al domicilio de la empresa: en la casa de cada empleado.
- Utilización de TICs para realizar el trabajo: notebook, celular, VPN, conexión a internet.
- Método de organización y ejecución de la actividad laboral: cada uno de los empleados, dependiendo del sector al que pertenezca deberá coordinar las actividades con su superior.

Recomendaciones de seguridad para el teletrabajador:

- Conectarse siempre a la VPN mediante redes privadas y seguras.
- Que la contraseña de sesión de la notebook cumpla con los requisitos mínimos de seguridad impuestos en la Política de Seguridad de la empresa.
- Que el celular posea factores biométricos para desbloquearlo.
- Permitir la actualización del sistema operativo de la notebook y del celular en cuanto estos dispositivos lo recomienden.
- No descargar programas que no sean de fuentes verídicas o páginas oficiales.
- Configurar el bloqueo automático en dispositivos luego de 10 minutos de actividad.
- Bloquear siempre los dispositivos cuando se dejen de usar o se pierdan de vista.
- Dejar habilitado el antivirus de los dispositivos en todo momento.
- Contactarse con el equipo de Seguridad Informática en caso de surgir algún incidente o tener alguna duda.

8. Conclusiones

Todo gran cambio merece grandes responsabilidades y grandes resultados. En este trabajo se detallaron todas aquellas responsabilidades y tareas que tendrán los equipos que sufrirán esta nueva modalidad de trabajo, desde los nuevos teletrabajadores hasta los equipos de Seguridad Informática y Sistemas que se harán cargo de la transición por completo. Se considera que este departamento está preparado y planificó las políticas y el programa de seguridad adecuados para comenzar con la implementación de este proyecto. A partir de este momento, la infraestructura de la empresa soportará modificaciones y se adaptará a todos los cambios logrando una nueva modalidad de trabajo mixta entre todos los empleados: empleados en oficinas y empleados en home-office.

Referencias Bibliográficas

[1] Las Claves del Éxito para la Gestión de Riesgos – ISOTools Excellence.

[2] Merce Molist (2014). El eslabón más débil en seguridad informática eres tú. https://www.elmundo.es/tecnologia/2014/01/18/52d-90707ca4741f2798b4570.html .

[3] 5 acciones para un proceso de Gestión de Riesgos eficaz. ISOTools Excellence. https://www.isotools.org/2017/10/08/5-acciones-proceso-de-gestion-de-riesgos-eficaz/#:~:text=Minimizar%20el%20impacto%20del%20riesgo,m%C3%ADnimo%20y%20f%C3%A1cil%20de%20subsanar .

[4] Software Backup Exec. Veritas. https://www.veritas.com/protection/backup-exec.

[5] Veritas Backup Exec. https://www.veritas.com/content/dam/Veritas/docs/data-sheets/V0276_GA_ENT_DS_BackupExec_20.1-EN.pdf.

[6] André Goujon (2012). ¿Qué es una VPN y cómo funciona para la privacidad de la información? https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/.