Melchor Mascaró

POLITICAS DE SEGURIDAD DE LA INFORMACION GRUPO MELCHOR MASCARÓ

Contenido 1 Objetivo

1 Objetivo

La dirección de MELCHOR MASCARÔ ha decidido establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) de acuerdo con la Norma UNE-ISO/IEC 27001:2013 dentro del contexto de los riesgos identificados por la Empresa. De esta manera se podrá determinar las necesidades que permitan proteger la Información a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, no repudio, disponibilidad, legalidad y confidencialidad de la información.

Los objetivos específicos que ha establecido para el cumplimiento de su misión, visión, objetivos estratégicos y alineados a sus valores corporativos, se establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

Cumplimiento, Según el requiso de la Norma UNE-ISO/IEC 27001 :2013 la Dirección debe asegurar que la Política de Seguridad es adecuada al propósito de la Empresa, incluye un compromiso de cumplir con los requisitos y de mejorar continuamente la eficacia del SCSI, proporciona un marco de referencia para establecer y revisar los objetivos del SGSI, es implantada, comunicada y entendida dentro de las áreas afectadas de la Empresa, es revisada para su continua adecuación, cumpliendo con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad.

Identificación y atención necesidades. Las personas que usan los recursos informáticos y las redes del GRUPO MELCHOR MASCARÓ son responsables de no abusar de estos recursos y de mantener el respeto a los derechos del resto de usuarios/as, así como proteger la información y los activos tecnológicos de la entidad. Esta política aporta una serie de recomendaciones y líneas de actuación para distinguir entre el uso correcto de los sistemas de información y el indebido.

Garantía de protección: Quien utilice nuestras redes y nuestros sistemas de información debe respetar la integridad de los recursos basados en los sistemas de información, evitar actividades destinadas a obtener accesos no autorizados o suplantación de identidad, respetar los derechos del resto de usuarios/as, no

acaparar en exceso recursos compartidos con el resto depersonas que los usan y respetar las políticas de licencias de software.

Confianza. Se pretende generar la confianza de la clientela con el compromiso de todos los miembros de la plantilla y personas colaboradoras de MELCHOR MASCARO respecto al correcto manejo y protección de la información que es gestionada y resguardada por nuestra entidad.

Se pretende concienciar al personal, empresas proveedoras y empresas clientes de MELCHOR MASCARO sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades diarias, garantizando la confidencialidad, Ila privacidad y la integridad de la información

2 Ámbito de aplicación

La Política de Seguridad de la Información aplica a todo el conjunto de las empresas que forman parte del grupo MELCHOR MASCARO, que tengan acceso a información a través de los documentos, equipos informáticos, infraestructura tecnológica y canales de comunicación de las empresas del Grupo.

Debido a las diferentes actividades de las entidades que forman parte de MELCHOR MASCARO, la Empresa considera necesaria la aplicación de la presente política de seguridad sobre todo el conjunto de los sistemas informáticos del grupo, atendiendo especialmente al servicio de archivo de historias clínicas.

2.1 Agentes a los que se aplica esta política

Esta política será de aplicación para todas las personas vinculadas con MELCHOR MASCARÓ ya sea personal de apoyo, personal de administración, equipo directivo, personas colaboradoras externas, becarias/os, etc., en cuanto a que hagan uso de los recursos expuestos en el siguiente apartado. También se aplicará a cualquier otra entidad externa que utilice los recursos informáticos de la Empresa.

2.2 Recursos a los que se refiere esta política

Se incluyen aquí todos los sistemas de información del GRUPO MELCHOR MASCARÓ ya sean individuales o compartidos y estén o no conectados a nuestras redes. Se aplicará a todos los equipos (estaciones de trabajo, PC's y servidores, dispositivos portátiles y telefonía móvil) e infraestructura de comunicaciones que sean propiedad o estén administrados por GRUPO MELCHOR MASCARÓ, así como aquellos equipos que se conecten a través de una extranet a las redes de la Empresa.

Todo esto incluye terminales, ordenadores personales, estaciones de trabajo, servidores y periféricos asociados, así como el software, independientemente de que se use para gestión administrativa, económica, comercial u otros.

2.3 Aspectos normativos y reglamentarios

Son de aplicación las leyes y normativa españolas, así como las que emanen de la Unión Europea y de las comunidades autonómicas en relación con protección de datos personales, propiedad intelectual y uso de herramientas telemáticas, así como las que puedan aparecer, en un futuro, a este respecto.

Esta política se sitúa dentro del marco jurídico definido por las leyes y reales decretos siguientes:

- Norma UNE-ISO/IEC 27001:2013 Norma de Sistemas de Gestión de la Seguridad de la Información.

- UNE-ISO/IEC 27002 - Tecnología de la Información. Código de buenas prácticas para la gestión de la Seguridad de la Información.

- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la intimidad Personal y Familiar y a la Propia Imagen,

- Ley Orgánica de Protección de Datos (15/1999) y Reglamento de desarrollo de la Ley Orgánica (RD 1720/2007)

- Ley de Servicios de la Sociedad de la Información (de 12 de octubre de 2002)

- Reglamento General de Protección de Datos (UE) 2016/679

3 Justificación

Los ordenadores y la red proporcionan acceso y recursos y nos permiten la comunicación con usuarios/as en todo el mundo. Este privilegio acarrea unas responsabilidades a las personas que los usan, que han de respetar los derechos de los otros que también lo hacen, la integridad del sistema y de los recursos físicos y respetar las leyes y regulaciones vigentes.

3,1 ¿Qué es la Seguridad de la Información?

La información es un activo que, como otros activos importantes del negocio, tiene valor para la Empresa y requiere en consecuencia una protección adecuada, La seguridad de la información protege a ésta de un amplio elenco de amenazas para asegurar la continuidad del negocio, minimizar los daños a la Empresa y maximizar el retorno de las inversiones y las oportunidades de negocio.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en vídeos o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información se caracteriza aquí como la preservación de:

a) su confidencialidad, asegurando que sólo las personas que estén autorizadas puedan acceder a la información;

b) su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos;

c) su disponibilidad, asegurando que las personas autorizadas tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software, Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la Empresa.

3.2 ¿Por qué es necesaria la seguridad de información?

La información y los procesos que la apoyan, sistemas y redes son importantes activos de la Empresa. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, tesorería, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones, Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. La tendencia

hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de toda la plantilla de la Empresa. También puede requerir la participación de las empresas proveedoras, empresas clientes y accionistas.

3,3 Datos personales

La recogida de datos personales se realizará utilizando siempre los medios fijados por la empresa (impresos, formularios...), de forma que se garantice que la persona interesada recibe la información necesaria sobre el tratamiento de sus datos personales y que se recaben los consentimientos necesarios para los tratamientos a realizar y las posibles comunicaciones de datos que vayan a llevarse a cabo.

No se comunicarán datos personales a terceros sin el consentimiento del titular, salvo para el cumplimiento de obligaciones legales (Agencia Tributaria, Seguridad Social, jueces, etc.) o que el acceso a los datos sea necesario para la prestación de un servicio contratado por la Empresa, siempre y cuando dicho acceso esté regulado en el contrato.

4 Políticas de buenas prácticas de Seguridad de la Información

A continuación, se plantean una serie de recomendaciones que pretenden regular el buen uso, disponibilidad y nivel de servicio de los recursos informáticos de MELCHOR MASCARO. Aquellas personas que de forma reiterada o deliberada

o por negligencia las ignoren o las infrinjan, se podrán ver sujetas a las actuaciones técnicas (para minimizar 'los efectos de la incidencia) o disciplinarias que se estimen oportunas,

Ud, debe velar por la confidencialidad y seguridad de la información en sus actuaciones cotidianas.

Los sistemas informáticos y las comunicaciones solo pueden utilizarse para tareas directamente relacionadas con el puesto de trabajo.

4.1 Proceso de autorización de recursos para el tratamiento de la información

Cualquier persona que necesite un nuevo ordenador, portátil, software, etc. deberá remitir la solicitud al departamento de TIC, indicando claramente el motivo o necesidad de la compra. La persona responsable de TIC aceptará, denegará o remitirá al comité de dirección la petición.

4.2 Uso apropiado de los activos: Internet

Uso apropiado del servicio de Internet/Intranet

Los miembros de la plantilla con autorización al uso y acceso a estos servicios deben:

- El acceso a Internet está limitado a uso estrictamente relacionado con la actividad profesional, por lo que sólo se puede hacer uso de este servicio para fines laborales.
- Conservar normas de respeto, confidencialidad y criterio ético en el uso de este servicio.

- Descargar documentos o archivo tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

Uso indebido del servicio de Internet/Intranet:

Acceder a sitios de juegos o apuestas en línea.

No se permite el uso de sistemas de búsqueda y obtención de archivos de música, videos o archivos comerciales con derechos reservados.

Acceder a sitios de divulgación, descarga o distribución de películas, videos, música, real audio, webcams, emisoras online, etc.

Acceder y/o descargar material pornográfico u ofensivo.

Utilizar software o servicios de Correo electrónico (chat) y redes sociales no instalados o autorizados por el Grupo de Soporte Tecnológico.

Compartir en sitios web información propia de MELCHOR MASCARO clasificada como reservada o confidencial.

- Emplear este servicio para la recepción, envió o distribución de información pública clasificada o reservada de MELCHOR MASCARO a través de servicios y cuentas de correo públicos.
- Realizar intentos no autorizados para acceder a otra cuenta de usuario/a de este servicio.
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de propiedad intelectual.
- Utilizar el servicio de Internet/Intranet para propósitos comerciales ajenos a MELCHOR MASCARO.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por MELCHOR MASCARO.
- Interferir intencionalmente con la operación normal de cualquier website o portal en Internet.
- Comprar o vender artículos personales a través de sitios web o de subastas en línea.

- Acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo de canal de comunicaciones. Únicamente se autorizará el acceso a aquel personal que por sus actividades requieran realizar este tipo de actividades.

- Publicar o enviar opiniones personales, declaraciones políticas y asuntos no propios del MELCHOR MASCARO,

- Descargar, instalar y configurar navegadores distintos a los permitidos por el Dpto.

Responsabilidades del uso de Internet/lntranet en MELCHOR MASCARO:

- Conocer, adoptar y acatar esta política cada vez que haga uso de este servicio.

- No se dispone de privilegios para la instalación de software

- Usar correctamente sus contraseñas (usuario y clave). La cuenta de acceso que proporciona MELCHOR MASCARO es personal e intransferible, por lo que no debe proporcionarse a otras personas.

- Dar aviso al Dpto. TIC a través de los medios establecidos de cualquier fallo de seguridad de su cuenta, incluyendo su uso no autorizado, pérdida de la contraseña, bloqueo, etc.

- Proteger los derechos de autor de la información obtenida a través de este servicio. Se recomienda citar la fuente (página web) en los documentos o informes generados con información obtenida por este medio.

- El personal ha de ser consciente de que el GRUPO MELCHOR MASCARÓ, sí puede conocer el contenido de la información que circula a través de su red y conocer que se registran por cada usuario/a las visitas a los diferentes sitios y webs.

- El Dpto. TIC planifica periódicamente una revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas y navegación en Internet-lntranet.

4.3 Extracción de pertenencias

Los equipos, la información o el software no se pueden sacar fuera de las instalaciones. Para realizar reparaciones, el personal técnico se desplazará a la ubicación del equipo averiado.

El uso de medios de almacenamiento externo en los diferentes equipos y unidades de red compartidas y servidores de la entidad, constituyen una herramienta que sirve para la transferencia rápida y directa de información entre el personal y las personas colaboradoras que a la vez puede exponer información confidencial y sensible de la entidad a diversos riesgos y peligros.

MELCHOR MASCARO es consciente de que este tipo de herramientas son muy útiles para el resguardo y transporte de información pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción; Por esta razón MELCHOR MASCARO define los compromisos frente al uso de Dispositivos de Almacenamiento Externo para asegurarse de que la información propietaria, adquirida o puesta en custodia en la entidad no está supeditada a fuga, uso no autorizado, modificación, divulgación o pérdida y que esta debe ser protegida adecuadamente según su valor, confidencialidad e importancia,

El uso de dispositivos de almacenamiento externo está permitido en MELCHOR MASCARO para su personal, con el fin de facilitar el compartir y transportar información que no sea de carácter clasificado ni reservado de la Institución dentro de las normas y responsabilidades del manejo de información institucional.

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos, mediante una conexión inalámbrica directa a cualquier equipo de cómputo de MELCHOR MASCARO.

Uso indebido de dispositivos de almacenamiento externo:

- Almacenar o transportar información clasificada o reservada de MELCHOR MASCARO sin la debida autorización y con las debidas salvaguardas de su seguridad.

- Ejecutar cualquier tipo de programa no autorizado por MELCHOR MASCARO desde cualquiera de las unidades de almacenamiento en mención.

- Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos. Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del usuario/a de alguno de estos medios de almacenamiento.

- Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información sensible o reservada del personal usuario de la empresa.

Responsabilidades en el uso de dispositivos de almacenamiento externo:

- Usar de manera responsable la información a su cargo y de los dispositivos de almacenamiento externo que emplee para el transporte de dicha información.

- Velar porque los medios de almacenamiento externo estén libres de software malicioso, espía o virus para lo cual deberá realizar una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la Institución por medio del software de protección dispuesto para tal fin.

- Toda la actividad realizada con dispositivos de almacenamiento externo, conectados a cualquier equipo de cómputo de la institución, podrán ser auditados con el ánimo de registrar y controlar las actividades realizadas sobre cada uno de estos, la ubicación y quien los empleó. Los intentos de habilitar el uso de estos dispositivos donde su uso ha sido denegado o no autorizado igualmente podrán ser registrados.

- Las entradas de software malintencionado, de espionaje o virus podrán ser detectadas inmediatamente e informadas al administrador de la red de MELCHOR MASCARO.

Se pueden generar informes periódicos sobre el uso de todos los elementos en MELCHOR MASCARO para permitir la evaluación del "uso racional de los dispositivos" y que estos sean permitidos, a fin de incrementar los niveles de seguridad para proteger la información de la empresa.

4.4 Derechos de propiedad intelectual.

El personal usuario y administrador debe respetar las condiciones de licencia y copyright del software que usen en sus equipos.

Todo software que se use en MELCHOR MASCARO para fines administrativos o comerciales debe estar debidamente licenciado, con un número de licencias que se corresponda con el número de usuarios/as simultáneos. Por supuesto, podrá usarse en equipos de MELCHOR MASCARO software "libre"

Todo software que se use que esté protegido por Copyrights no puede ser copiado, salvo con autorización de su titular. No se podrán usar los medios que MELCHOR MASCARO pone a disposición de su comunidad para copiar software protegido o romper las protecciones del mismo.

Aparte del software, toda otra información que también posea derechos de autor, que esté en formato electrónico y que haya sido obtenida de otro equipo o red, se debe usar de acuerdo con la legislación vigente.

El personal responderá siempre personalmente del software que haya instalado en sus equipos, así como del uso que del mismo se efectúe, y deberán cumplir con las obligaciones y requisitos que se deriven de su instalación y utilización.

En ningún caso ningún miembro de la plantilla podrá permitir que ninguna persona lleve a cabo la instalación en sus equipos de software que no esté debidamente licenciado.

4.5 Controles contra el código malicioso

Está instalado en los servidores un software detector de código malicioso. Se ejecuta un control de detección como mínimo una vez por semana.

4.6 Correo electrónico y envío de mensajes

Uso apropiado del servicio del Correo electrónico, Cualquier miembro del personal que lo haya solicitado al Dpto. de TIC y se le haya aprobado dispone de una cuenta de Correo electrónico activa, protegida con código de usuario y

contraseña la cual puede utilizar desde los diversos equipos destinados para ello y únicamente para uso profesional, por lo que es de su responsabilidad hacer buen uso de su cuenta, entendiendo por buen uso:

- Usar el servicio de Correo electrónico institucional exclusivamente para fines laborales, siendo el uso de su cuenta con fines comerciales o de producción de interés para MELCHOR MASCARO.

- Transferir archivos que no tengan información sensible o reservada de MELCHOR MASCARO. Se debe revisar previamente que cualquier archivo a enviar esté libre de virus.

- Abstenerse de compartir información o datos personales a través de este servicio.

- Compartir por medio de este canal mensajes concisos, breves y veraces, haciendo uso de un lenguaje apropiado en sus comunicaciones.

- Mantener su estado actualizado en el sistema de modo que los demás usuarios sepan si están o no disponibles y si pueden o no contactarle.

- Leer diariamente su correo y obligatoriamente guardar una copia fuera del Outlook de aquellos correos que puedan considerarse relevantes para futuras gestiones laborales,
- No permitir que terceras personas hagan uso de su cuenta.

Uso indebido del servicio de Correo electrónico:

Está estrictamente prohibido el uso de la cuenta para fines personales

Expresar opiniones difamatorias, ofensivas, obscenas, vulgar, racistas, calumniadoras y sexuales sobre superiores, compañeros/as o subalternos. Lo mismo aplica para personas usuarias, empresas proveedoras y demás entidades con quien haya comunicación.

Enviar SPAMS de información (correo basura), o enviar anexos (attachments) que pudieran contener información nociva para otro usuario/a como virus o pornografía

- Abrir correo con archivos adjuntos sospechosos
- El mandar o contestar cadenas de correo
- Emplear las comunicaciones instantáneas con fines políticos, religiosos o comerciales ajenas a la actividad de la empresa,
- Realizar cualquier tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.
- Compartir por medio de este canal información clasificada o reservada de MELCHOR MASCARO o de su plantilla o entidades colaboradoras.
- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Compartir documentos o archivos que sean ajenos a la operación de MELCHOR MASCARO.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de las empresas clientes de Correo electrónico instalados por MELCHOR MASCARO.

- Descargar, instalar y emplear sistemas de Correo electrónico distintos al definido por MELCHOR MASCARO y administrado por el Dpto. TIC. Los sistemas no autorizados incluyen, pero no se limitan a: Yahoo! Messenger, AOL Instant Messenger (AIM), MSN Messenger, Whatsapp, eBuddy, ICQ, MySpace y Google Talk.

- El uso inapropiado o el abuso en el servicio de Correo electrónico puede ocasionar la desactivación temporal o permanente de las cuentas.

Responsabilidades de los trabajadores y usuarios del servicio de Correo electrónico:

- Conocer, adoptar y acatar este lineamiento cada vez que haga uso de este servicio.

- Usar correctamente sus contraseñas de acceso (usuario y clave). La cuenta de acceso que proporciona MELCHOR MASCARO es personal e intransferible, por lo que no debe proporcionarse a otras personas.

- Dar aviso al Dpto. TIC, a través de los medios establecidos, de cualquier fallo de seguridad de su cuenta, incluyendo su uso no autorizado, olvido de la contraseña, bloqueo, etc.

- Cuando se remitan e-mails masivos con copia a otros destinatarios/as se utilizará siempre la opción de copia oculta (CCO...), salvo el caso de correo interno.

Todos los mensajes compartidos y documentos archivos compartidos o descargados quedan bajo responsabilidad de la persona dueña de la cuenta.

Cada jefatura de área es responsable de revisar y autorizar o desautorizar cada requerimiento de acceso del personal bajo su responsabilidad a este servicio. Solicitudes aprobadas de acceso deben ser sometidas de acuerdo con el procedimiento vigente para este caso.

- El personal deben ser conscientes de que se registra y se puede acceder a los mensajes enviados y recibidos y pueden ser auditados tanto los equipos facilitados para su uso profesional como en los servidores donde se administran estos servicios.

- El Dpto. TIC planifica periódicamente una revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas

4.7 Sistemas de información del negocio

El correo ordinario solo podrá ser abierto por el personal AUTORIZADO, quien lo distribuirá sin abrir a la persona a la que vaya indicada.

Las transmisiones de fax recibidas se entregarán de inmediato al destinatario/a por el personal autorizado.

4,8 Política de puesto de trabajo despejado y pantalla limpia

Los puestos de trabajo están protegidos con un bloqueo automático de la pantalla controlado por contraseña.

La política de escritorios y pantallas despejadas es extensiva para todo el personal de MELCHOR MASCARO y se apoya en la seguridad de la información sensible o crítica de la empresa.

El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los miembros de la plantilla que tengan acceso a la información de MELCHOR MASCARO, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades. Para su definición y aplicación se define de la siguiente manera:

Escritorios:

- Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información clasificada o reservada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.

- En la medida de lo posible los documentos con información clasificada o reservada debe quedar bajo llave o custodia en horas no laborables.

- Se debe evitar la salida de documentos clasificados o reservados de la institución y en el caso de ser necesario y con la debida autorización se debe garantizar su protección fuera de la empresa y su oportuna devolución.

- La información en papel cuando no se utiliza debe estar guardada en armarios cerrados con llave.

- Únicamente podrá archivarse información en las áreas previstas para ello y mediante los criterios establecidos por la empresa.

- No se dejará información abandonada, al alcance de terceras personas o personal ajeno al departamento.

Los dispositivos de fax y copiadoras están controlados por la persona responsable del área. Los documentos que se imprimen o copian en ellos son inmediatamente entregados a sus destinatarios/as.

Sólo está autorizado el uso de fax, impresoras y fotocopiadoras para uso profesional dentro la actividad de MELCHOR MASCARO.

- Se debe restringir la realización de fotocopias de documentos fuera del horario normal de trabajo y fuera de las instalaciones. De ser necesario se debe garantizar su protección y confidencialidad fuera de las mismas.

- Al imprimir o fotocopiar documentos con información clasificada o reservada, ésta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.

- No se debe enviar ni recibir documentos clasificados o reservados por medio de Fax.

- No se debe reutilizar papel que contenga información clasificada o reservada.

Pantallas:

- Los PCs deben ser bloqueados, al retirarse de los mismos y los éstos deben ser desbloqueados por medio del usuario y contraseña asignado para su acceso a los mismos. Es responsabilidad del usuario/a, asegurar que el equipo tenga la protección adecuada

4.9 Política de uso de los servicios de red interna.

Los objetivos específicos del uso de servicio de internet/intranet son:

- Incentivar el uso del servicio de Internet/Intranet para fines estrictamente laborales de MELCHOR MASCARO y para aquellos que se puedan considerar de interés para el personal de la empresa.

- Asegurar el correcto manejo de la información privada de MELCHOR MASCARO.

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información a través de este servicio.

El servicio de Internet/Intranet es un servicio de gran importancia en el mundo laboral, de conocimiento y negocios basado en el acceso a diferentes fuentes de información en distintas ubicaciones a través de sistemas interconectados en red a nivel local y mundial.

El acceso al servicio de Internet/Intranet es un permiso otorgado por MELCHOR MASCARO a su personal y así mismo sobrelleva responsabilidades y compromisos para su uso. Se espera que los usuarios/as de este servicio conserven normas de buen uso, confidencialidad y criterio ético.

Solo se dispondrá de acceso a las carpetas compartidas en las que se tiene permisos asignados, previamente autorizados por el responsable de TIC.

Uso apropiado del servicio de Intranet

Todo el personal con autorización al uso y acceso a estos servicios debe:

- Utilizar este servicio exclusivamente para fines laborales o para aquellos que puedan ser considerados de interés para el personal de Melchor Mascaró.

Conservar normas de respeto, confidencialidad y criterio ético por parte de todas aquellas personas con acceso a este servicio.

- Descargar documentos o archivo tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

Uso indebido del servicio de Intranet:

- Compartir información de MELCHOR MASCARO clasificada como reservada, o cualquier información con personas no autorizadas para ello.

- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.

- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por MELCHOR MASCARO.

- Publicar o enviar opiniones personales, declaraciones políticas y asuntos no propios de MELCHOR MASCARO, dirigidos a terceras personas, a través de este servicio.

Responsabilidades derivado del uso de Intranet en MELCHOR MASCARO:

- Conocer, adoptar y acatar esta política cada vez que haga uso de este servicio.

- Usar correctamente sus contraseñas de acceso (usuario y clave). La cuenta de acceso que proporciona MELCHOR MASCARO es personal e intransferible, por lo que no debe proporcionarse a otras personas.

- Dar aviso al Dpto. TIC a través de los medios establecidos de cualquier fallo de seguridad de su cuenta, incluyendo su uso no autorizado, pérdida de la contraseña, bloqueo, etc.

- Proteger los derechos de autor de la información obtenida a través de este servicio,

- Todo el personal debe ser conscientes de que se registra por cada usuario/a las visitas a los diferentes sitios y se registran estos eventos en archivos de auditoria tanto en los PCs como en los servidores donde se administran estos servicios.

- El Dpto. TIC planifica periódicamente una revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas y navegación en Intranet.

4.10 Sistema de gestión de contraseñas

Las contraseñas ofrecen un medio de validar la identidad de cada usuario/a, pudiendo así establecer los derechos de acceso a los recursos o servicios de tratamiento de la información.

Todo el personal se compromete a:

Mantener la confidencialidad de las contraseñas;

Evitar la escritura de las contraseñas en papel, salvo si existe una forma segura de guardarlo;

Cambiar las contraseñas si se tiene algún indicio de su vulnerabilidad o de la del sistema;

Seleccionar contraseñas de buena calidad, con una longitud mínima de 6 caracteres, que cumplan con las siguientes condiciones: - La clave contenga letras mayúsculas y minúsculas

- Este compuesta por letras y números

- No estén basadas en algo que cualquiera pueda adivinar u obtener usando información relacionada con el usuario/a, por ejemplo, nombres, fechas de nacimiento, números de teléfono, etc.

Cambiar las contraseñas temporales asignadas para inicio, la primera vez que se acceda al sistema,

No incluir contraseñas en ningún procedimiento automático de conexión, que, por ejemplo, las almacene en una macro;

No compartir contraseñas de usuario/as individuales

No apuntar contraseñas en dispositivos móviles, agendas, etc.

Cada 25 días se debe cambiar obligatoriamente la contraseña No se pueden repetir las 24 últimas contraseñas.

Se bloquear a los 3 intentos.

Cada persona es responsable de su clave de acceso al sistema y aplicaciones (en caso de tener una). Las acciones realizadas con una determinada clave serán responsabilidad de la persona a la que esté asignada. No se abandonarán los puestos de trabajo con sesiones de usuarios abiertas, siendo necesaria una nueva identificación siempre que alguien intente acceder a un equipo.

4.11 Ordenadores y comunicaciones móviles.

La política de uso de dispositivos móviles teléfonos, ordenadores portátiles y tablets aplica a todo el personal y entidades colaboradoras de MELCHOR

MASCARO y apoya la seguridad de la información sensible o crítica de MELCHOR MASCARO,

Los objetivos específicos de este capítulo relacionado con el uso de dispositivos móviles son:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.

- Crear conciencia sobre los riegos asociados al manejo de información a través de las Tablets y teléfonos y la manera de reducirlos.

- Especificar las recomendaciones y pautas necesarias para mantener tanto los dispositivos como la información protegida.

- Dictar las pautas para mantener la operación, y transmisión de la información registrada en las tablets y teléfonos móviles.

Responsabilidades del Dpto. TIC:

- Determinar y avalar las opciones de protección de los dispositivos móviles institucionales que hagan uso de los servicios provistos por MELCHOR MASCARO.

- Establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por MELCHOR MASCARO.

- Determinar los métodos de protección de acceso (por ejemplo, contraseñas o patrones) para los dispositivos móviles institucionales que serán entregados al

personal. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

- Activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles de la empresa haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo,

- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

- Implementar una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse a la Política de Copias de Respaldo.

- Instalar un software de antivirus en los dispositivos móviles institucionales que hagan uso de los servicios provistos por MELCHOR MASCARO.

- Activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos y almacenar estos códigos en un lugar seguro.

Responsabilidades del personal:

- Se debe evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

- No deben modificarse las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega,

- Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

- Aceptar y aplicar la nueva versión de las actualizaciones que sean notificadas en los dispositivos móviles asignados para su uso, Evitar hacer uso de redes inalámbricas de uso público, así como se deben desactivar las redes inalámbricas como WIFI, Bluetoothl o infrarrojos en los dispositivos móviles asignados.

Evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

- Abstenerse de almacenar videos, fotografías o información personal en los dispositivos móviles asignados.

4.12 Teletrabajo

Puntualmente, en caso de necesidad, se puede realizar teletrabajo a través de un escritorio remoto.

Las políticas de seguridad que rigen para Terminal Server son las mismas que rigen internamente en la Empresa.

4.13 Proceso disciplinario

En caso que fuera necesario, corresponderá a Dirección la adopción de medidas disciplinarias ante infracciones de esta política, una vez informado por la persona Responsable de Seguridad.

4.14 Seguridad de los equipos fuera de los locales de la Empresa

Ver punto 5.3 y 5.1 1

5 Otras políticas de seguridad de la información

5.1 Buenas prácticas para el trasporte y custodia de los archivos

Las claves para la desconexión de la alarma de las instalaciones del archivo son personales e intransferibles que disponen algunas personas

El acceso al programa informático y ordenadores está restringido a determinadas personas autorizadas por ser su herramienta de trabajo habitual, en el caso de que alguna persona por algún determinado necesitara utilizar el ordenador será bajo la autorización del responsable Dpto. TIC

La puerta de acceso al archivo permanecerá siempre cerrada, no permitiéndose acceso a terceras personas no autorizadas. De ser necesario el acceso de no autorizados se llevará un registro de los accesos.

Para los servicios de expurgo de documentación las cajas deberán precintarse siempre en las instalaciones de la empresa cliente. En el caso de custodia de archivos dependerá del servicio contratado.

En todos los procesos de transporte de archivos, se transportarán en cajas selladas y cerradas. Después de la carga y la descarga de los archivos, todas las puertas de los vehículos utilizados deberán cerrarse inmediatamente con llave y los archivos que queden por entregar no se quedarán en lugar visible.

Únicamente podrán realizar tratamientos de datos fuera de la empresa el personal autorizado expresamente para ello. Durante el transporte de documentos o soportes deberán adoptarse medidas para evitar el acceso no autorizado a los datos tales como sobres, maletines o cajas cerradas, o cualquier medida equivalente.

6 Registro de Incidencias

Cualquier incidencia que afecte a la seguridad de la información, a su confidencialidad o a su integridad, deberá ser notificada a la persona responsable de su departamento y/o al DPTO TIC, quien a su vez deberá registrarla en el registro de incidencias existente.

7 Destrucción de la información

Para desechar cualquier papel que contenga información personal, aunque solo sean nombres de pila, deberá hacerse uso de una destructora de papel o contenedor de documentos confidencial, en caso de disponer de uno.

8 Protección de datos de carácter personal.

En caso de recibir una solicitud de ejercicio de los derechos reconocidos por la LOPD y RGPD, informar inmediatamente a la persona Responsable para la atención a los derechos del afectado.

Deben seguirse las Instrucciones que se reciban de Dirección en materia de datos personal y seguridad de la información.

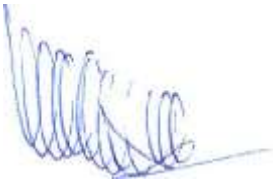
Ante cualquier duda, preguntar a la persona responsable de su departamento o

a la dirección,

Manacor 8 de agosto de 2018

Dª Antonia Mascaró Martorell

D. Juan Mascaró Martorell



Dª Maria Mascaró Martorell

D. Jaime Mascaró Martorell