Management Solutions

Política de Seguridad

0. INTRODUCCIÓN

El objetivo de la Política de Seguridad es establecer los principios de seguridad de la información y de los Sistemas frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. La Política engloba tanto la seguridad física de las instalaciones de la Firma como la seguridad lógica del Entorno Informático disponible.

La Política de Seguridad y el Sistema de Gestión de Seguridad de la Información (SGSI) en el que se enmarca están sujetos a revisión constante y mejora continua. Tanto la política como los manuales, procesos y registros asociados se revisarán con carácter anual, a efectos de mantenerlos convenientemente actualizados. Así mismo se efectuará toda modificación necesaria en función de posibles cambios que puedan derivar de dicha actualización: cambios tecnológicos, plan de pruebas, plan de auditorías, etc.

1. OBLIGACIÓN DE CONOCER Y CUMPLIR

Todo profesional de la Firma, independientemente de su posición y función, está vinculado con esta Política de Seguridad (en adelante, 'la Política'). En consecuencia, debe mantenerse actualizado con la última versión disponible en la Intranet y actuar conforme a los principios definidos, comunicando a su responsable directo o al CISO cualquier duda respecto a su contenido.

Todos los directivos tienen obligación de comunicar el contenido de esta Política a sus equipos, liderar su cumplimiento, resolver las dudas o inquietudes que les transmitan los profesionales, y establecer los mecanismos que aseguren su cumplimiento.

El incumplimiento de las normas contenidas en la presente Política estará sujeto a la potestad disciplinaria y sancionadora de la Firma, de acuerdo a los principios y reglas previstas por la legislación vigente. En este sentido, cualquier incumplimiento identificado tanto de las políticas internas o como de la normativa vigente en los países en los que opera la Firma, se debe comunicar al QA Global (bien comunicándose directamente con él o bien mediante el canal ético de la Firma), quien se asegurará de aplicar los criterios de independencia, objetividad, confidencialidad, protección de datos, secreto de las comunicaciones y ausencia de represalias para el informante de buena fe, tal y como especifica la Política de Gestión de Dudas e Incumplimientos.

2. ÁMBITO DE APLICACIÓN

La presente política aplica a todos los profesionales que forman Management Solutions, con independencia de la modalidad contractual que determine su relación laboral, posición, o ámbito geográfico en el que desempeñen su trabajo (incluidos los estudiantes en prácticas).

El ámbito de aplicación se podrá también hacer extensivo a cualquier otro profesional vinculado con Management Solutions (colaborador puntual) cuya actuación pueda suponer un riesgo tecnológico para la Firma. De esta forma la política se aplica a todos los profesionales de MS y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Las medidas y disposiciones que se indican en el presente documento, deben ser complementarias y no eximentes, con las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos de carácter personal que cada país, en los que MS tiene representación, haya legislado oportunamente.

En concreto, estas medidas son complementarias a lo dispuesto en la normativa del Parlamento Europeo aprobada en abril de 2016 (2016/679) relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos (GDPR, aplicable a partir del 25 de mayo de 2018), así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD GDD) aprobada por el gobierno de España.

3. ROLES INVOLUCRADOS

El éxito en la aplicación de la política de seguridad se apoya en la distribución de funciones y responsabilidades, de forma que se establezca un marco gerencial para iniciar y controlar su implementación adecuada. A continuación, se detallan los roles involucrados y sus principales competencias:

Responsable de Seguridad Corporativo

El Responsable de Seguridad Corporativo es el promotor de las políticas de seguridad y de asegurar su cumplimiento en toda la Firma, combinando las directrices globales requeridas con las particularidades locales de cada Unidad.

Adicionalmente el responsable de Seguridad podrá contar con Responsable de Seguridad Física y Responsable de Seguridad Informática.

Responsables de Seguridad Local

Cada Unidad en la que opera la Firma dispone de un Responsable de Seguridad local, responsable de hacer cumplir la política en su ámbito de operación a través de la ejecución de controles establecidos y del reporte de las incidencias ocurridas.

Dichos controles y reporte de incidencias se realizan al Responsable de Seguridad que corresponda, según refiera seguridad física o informática.

Comité de Seguridad Informática y Asesores Externos

El Responsable de Seguridad Corporativo se apoyará en diversos especialistas para asegurar la adecuación, actualización y efectividad de las políticas definidas, así como su cumplimiento:

- Asesores externos: Mediante la realización de auditorías externas revisa que permitan evaluar la robustez de los sistemas de información en las que se incluyen, entre otras, test de intrusión, hacking ético o análisis de tráfico, emitiendo un completo informe al respecto.
- Comité de Seguridad Informática: Mediante la participación de profesionales experimentados de la Firma que propongan medidas y sugerencias vinculados, entre otros a:
    - **Cumplimiento**: la función de cumplimiento valorará, con la periodicidad que establezca el Responsable de Seguridad, si las medidas de seguridad establecidas son cumplidas con rigor. Cualquier fallo o incumplimiento detectado en cualquiera de dichas medidas se refleja en un informe asociado detallando el mismo e indicando el nivel de riesgo sobre la información afectada.
    - **Producción**: el responsable de la administración, mantenimiento y operación de los sistemas de la firma, cuya principal responsabilidad en este ámbito es asegurar y reportar la continuidad de las operaciones desde el punto de vista tecnológico.
    - **Desarrollo**: el responsable del departamento de desarrollo, cuya principal responsabilidad en este ámbito es sugerir, recibir, comprender y ejecutar los requerimientos de seguridad que emanen del Comité en lo referente a los desarrollos internos realizados en la Firma.
- Mejora Continua: Con periodicidad mínimo trimestral el Responsable de Seguridad Informática convocará al Comité de Seguridad Informática compuesto por un equipo de profesionales experimentados cuya responsabilidad es identificar las debilidades en política de seguridad, con riesgos identificados y las mejoras correspondientes.

Responsable de RRHH

Notificar a todo el personal que ingresa en MS de sus obligaciones respecto del cumplimiento de la Política de Seguridad y de todas las normas, procedimientos y prácticas que de ella surjan. Así mismo, tendrá a su cargo la notificación de dicha política a todos los profesionales de MS, de los cambios que en ella se produzcan, la suscripción de los compromisos de confidencialidad que correspondan y las funciones de capacitación continua en materia de seguridad.

Responsable del área legal

Verificar el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos u otra documentación de MS con sus empleados y con terceros. Así mismo, asesorará en materia legal a MS, en lo que se refiere a la seguridad de la información.

Usuarios de la información y de los sistemas

Responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad vigente.

4. SEGURIDAD FÍSICA

El objetivo de la Seguridad física es tanto prevenir e impedir accesos no autorizados a instalaciones de MS (nuestras oficinas y la ubicación donde reside nuestros Centros de Proceso de Datos –CPDs-), prevenir y evitar cualquier incidente de nuestros profesionales, o realizar un buen uso del escritorio en el puesto de trabajo en lo relativo a documentos o pertenencias que pudieran conllevar un riesgo de seguridad.

4.1. Seguridad física de instalaciones de MS

Seguridad de acceso a Oficinas

La protección de acceso a las oficinas de la Firma se realiza mediante la disposición de diversas barreras o medidas de control físicas:

- Todos los edificios en los que se ubican las oficinas de MS dispondrán de vigilancia de seguridad y de tornos de acceso accesibles mediante tarjeta magnética y/o recepción para el control de visitas[1].
- El acceso a la propia oficina se realiza mediante la apertura de la puerta de entrada con tarjetas magnéticas o mediante la introducción de una clave. A cada oficina se asigna un Responsable del control de acceso que gestionará la entrega a los empleados autorizados del mecanismo requerido en cada caso (tarjeta / clave).
- En todas las oficinas se dispone de una recepción para el control de acceso por parte de terceros a las propias oficinas de MS independientemente de la existencia o no de la propia recepción de entrada al edificio. En ningún momento permanecerá abierta la puerta de acceso. En el caso de que, por avería, no funcione el sistema de cierre, la entrada estará vigilada en todo momento, hasta que se resuelva dicha avería.
- Ningún profesional podrá dar acceso a quien no se identifique como profesional de la Firma, sin la autorización del Responsable del control de acceso.

Cualquier incidencia relativa al acceso a las oficinas de la Firma se deberá notificar al Responsable de Seguridad Local, quien, a su vez, informará al Responsable de Servicios Generales.

Seguridad de los CPDs

[1] En caso contrario, el Country Head deberá implantar medidas sustitutivas y someterlas a la aprobación del Responsable de Seguridad Corporativo

Actualmente los servicios críticos corporativos (sistemas y comunicaciones) se encuentran alojados en Data Centers en formato de cloud privada, asegurando que los datos sujetos a LOPD estarán ubicados en aquellos países autorizados por la LOPD. En concreto, se dispone de una solución de 2 Data Centers (TierIV Gold+ Tier III como respaldo) en Alta Disponibilidad (con plan de recuperación ante desastres asociado).

4.2. Recomendaciones de Seguridad para los profesionales

Management Solutions considera que la seguridad de sus profesionales es un aspecto prioritario, por lo que establece una serie de recomendaciones basadas en nuestra propia experiencia como Firma y en las normas publicadas por algunos organismos públicos internacionales:

Recomendaciones generales

- Para los traslados en taxi, utilizar únicamente vehículos acreditados oficialmente, previamente reservados o ubicados en paradas de confianza de hoteles, centros de trabajo y centros comerciales. Se recomienda dejar todo el equipaje en el maletero para evitar llamar la atención de delincuentes que aprovechan los momentos en los que el vehículo se encuentra parado (semáforos, atascos, etc.) para romper las lunas y sustraer las pertenencias personales de los viajeros.
- No es aconsejable conducir de noche por carretera y en caso de existir alternativa es siempre más aconsejable utilizar las autopistas de peaje, así como las carreteras principales antes que las secundarias. Se recomienda el desplazamiento en coche privado no llamativo o taxi y, cuando sea posible, en grupo.
- Se recomienda no salir haciendo ostentación de joyas u objetos de valor (relojes, móviles, ropa de marca, etc.) y no llevar grandes sumas de dinero en efectivo.
- En caso de asalto se recomienda no ofrecer ninguna resistencia, incluso aunque los asaltantes sean menores, ya que podrían ir armados y encontrarse bajo los efectos de las drogas.
- En caso de recibir llamadas telefónicas amenazantes, no mantener la conversación, no proporcionar absolutamente ningún dato y colgar el teléfono a la mayor brevedad posible. Procurar fijarse en el número de teléfono desde el que se ha recibido la llamada.
- Evitar cajeros automáticos en lo posible y, si es necesario, buscar alguno que se encuentre en el interior de zonas más protegidas, como centros comerciales, y actuar con cautela y discreción.
- Evitar el turismo en zonas de playa poco habitadas, así como las excursiones de montaña en entornos remotos.
- En el caso de efectuar pagos con tarjetas de crédito, conviene realizar un atento seguimiento posterior de los extractos bancarios pues se dan algunos casos de clonación de tarjetas.
- Durante la estancia en hoteles, utilizar las cajas fuertes disponibles en la mayoría de las habitaciones.
- Para quienes contraten personal: pedir referencias del servicio doméstico y otros empleados.

Recomendaciones específicas

Con independencia de la aplicación general de las medidas del apartado anterior, es importante conocer las específicas que puedan ser necesarias en cada país. A continuación, se indica el enlace a cinco webs de organismos internacionales de máximo interés en esta materia. Esta información se puede ampliar consultando la página web del organismo nacional correspondiente o de la embajada cada país.

- Ministerio de Asuntos Exteriores de España.
- Gov.UK.
- Travel.State.Gov.
- Portal das Comunidades Portuguesas.
- Auswaertiges amt.

Es conveniente releerlas periódicamente porque son recomendaciones que se van actualizando en función de las circunstancias de cada momento.

4.3.

4.4. Seguridad de escritorio despejado

Con el objetivo de garantizar la seguridad de la información, mantener un entorno de trabajo ordenado y promover la eficiencia operativa, Management Solutions establece la política que todos los empleados deben asegurarse de que sus escritorios estén libres de documentos confidenciales, dispositivos electrónicos, credenciales de acceso y otros objetos sensibles al final de cada jornada laboral o al ausentarse por periodos prolongados. Todo material importante deberá guardarse en cajones con llave, archivadores o sistemas digitales seguros. Esta práctica contribuye a proteger datos críticos, facilita la limpieza del área de trabajo y proyecta una imagen profesional ante clientes y colaboradores.

5. SEGURIDAD LÓGICA DE LA INFORMACIÓN

La seguridad lógica de la información y de los Recursos Informáticos de la Firma se articula a través del establecimiento de directrices en relación al Control de acceso a los sistemas, a la Seguridad de las Comunicaciones, y al Uso que los profesionales den a los mismos.

5.1. Control de Acceso a Sistemas

El objetivo principal es establecer los protocolos necesarios en el acceso a los sistemas de la Firma, de forma que se impida el acceso no autorizado a la información. Se disponen por lo tanto normas específicas en relación a:

Administración de usuarios

El proceso de alta y eliminación de usuarios se realiza por parte de los administradores del sistema, tras la comunicación por parte de la Dirección de RRHH. Se establecen mecanismos que aseguran que el personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones, y se definen mecanismos de gestión de privilegios a nivel grupo o perfiles de usuario evitando asignación a usuarios individuales.

Identificación y autenticación de los profesionales

Cualquier acceso a los ordenadores de la Firma se realiza utilizando un identificador único de usuario convenientemente autorizado y provisto de su correspondiente contraseña y factor múltiple de autenticación. El identificador en ningún caso podrá ser comunicado y/o cedido a un tercero. Así mismo, se establecen una serie de mínimos de calidad en relación a la calidad y confidencialidad de las contraseñas con objeto de asegurar un nivel adecuado de seguridad de las mismas. Los router MiFi y móviles corporativos se suministran con PIN inicial. Estos últimos, adicionalmente se entregan securizados mediante activación del sistema MDM.

Autorizaciones específicas

En caso de requerirse autorizaciones específicas (tanto de nuevos recursos de procesamiento de información como de acceso por parte de terceros a cualquier recurso tecnológico de la firma), dicha autorización deberá ser emitida por el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las políticas y requerimientos de seguridad pertinentes:

- Nuevos recursos tecnológicos – El Responsable de Seguridad Informática deberá considerar su propósito y uso antes de proceder a su autorización, especificando cualquier control adicional requerido.
- Acceso por parte de terceros – Evaluando junto con el propietario de la información afectada los riesgos asociados, identificando los controles específicos requeridos. Así mismo, en todos los contratos cuya prestación de servicios se realice dentro de MS, se establecen compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos otorgados. En ningún caso se otorgan accesos a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta que se han implementado los controles apropiados y se ha firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

5.2. Gestión de los Sistemas y de las Comunicaciones

El objetivo es garantizar la seguridad de la información asegurando el funcionamiento correcto de los sistemas de información de MS a través de una gestión eficiente y segura de los sistemas informáticos y de comunicaciones que lo componen, articulando medidas concretas de seguridad en relación a los siguientes ámbitos:

- Controles contra el software malicioso (firewall, proxy, antivirus, sistema EDR, antispam, permisos de administración restringidos, control e inventario de software instalado, etc.)
- Seguridad de las comunicaciones
- Cifrado de ordenadores personales
- Encriptación de soportes de información para su transporte. En el caso de soportes que almacenen información de Confidencialidad reforzada o Máxima confidencialidad, las medidas de seguridad se podrán reforzar a criterio del socio responsable
- Seguridad de instalación de software en los servidores
- Copias de seguridad de la información contenida en los sistemas
- Administración de medios informáticos removibles (no estando permitido el uso como norma general de memorias USB, discos duros externos, cd's o dvd's, etc…). En el caso de soportes que almacenen información de Confidencialidad reforzada o Máxima confidencialidad, las medidas de seguridad se podrán reforzar a criterio del socio responsable
- Eliminación de los medios de información (toda información confidencial en formato físico se debe destruir mediante contenedores de destrucción específicos disponibles en las oficinas o en su defecto destructores de papel). En el caso de medios de información de Confidencialidad reforzada o Máxima confidencialidad, las medidas de seguridad se podrán reforzar a criterio del socio responsable
- Administración remota y securización de los terminales móviles mediante el uso de un sistema MDM.

5.3. Normativa de Uso

El personal de MS debe cumplir con la normativa de uso de los recursos tecnológicos de la firma, con objeto de asegurar la seguridad y la confidencialidad de la información a tratar:

- Destino – Los sistemas de información se deberán utilizar con el único objetivo de cumplir sus funciones dentro de la empresa, no utilizando los sistemas ni la información tratada por los mismos para otros fines diferentes.
- Confidencialidad – No se compartirá ni el usuario ni la contraseña asignada a cualquier recurso de la Firma, ni se utilizará de forma fraudulenta para acceder a información a los que no se ha concedido autorización. La única circunstancia en la que se permite la cesión de contraseña es cuando lo requiera el personal de IT para poder realizar las funciones de soporte correspondiente. Cuando esto suceda y una vez finalizada la intervención por parte del personal de IT, se obligará al usuario a cambiar la contraseña. Las consecuencias que se deriven del incumplimiento de esta norma, serán de exclusiva responsabilidad del propietario del identificador del usuario.
- Veracidad – Velarán por que los datos de los sistemas son veraces, exactos y completos.
- Deber de custodia – Es obligación del profesional custodiar con diligencia los dispositivos corporativos facilitados por la Firma (ordenadores, móviles, etc.), no dejándolos sin supervisión en ningún momento (p.e. en restaurantes, medios de transporte, dejándolos lejos del contacto visual de un tercero en el coche particular, etc.).
- Notificación de incidencias – Notificarán mediante el envío al buzón incidenciasms@managementsolutions.com cualquier incidencia ocurrida en la seguridad de la información y/o en el funcionamiento de los recursos informáticos de la Firma.
- Uso del correo electrónico e Internet:
    - El uso deberá ser exclusivamente profesional, no estando autorizado el envío de documentación confidencial sin protección específica (cifrado, encriptación), envío de cartas en cadena, etc.
    - Se llevará a cabo una limitación de la navegación mediante la elaboración de listas negras identificadas a nivel de proxy corporativo y Microsoft *Edge*. En el caso de usuarios que tengan acceso a información de máxima confidencialidad, se procederá a la limitación de la navegación mediante el uso de listas blancas a través del proxy corporativo y Microsoft *Edge.*
    - Se realizará una monitorización del uso de las normas del correcto uso del correo electrónico y de la navegación por internet, siendo el tiempo de retención para este último, 90 días.
    - En el caso de perfiles que accedan a información de confidencialidad reforzada o de máxima confidencialidad, se podrá proceder a implementar medidas más restrictivas a criterio del socio responsable del proyecto.
- Instalación o uso de software – No está permitida la instalación de software en dispositivos corporativos ni el uso de software portable ajeno a la plataforma corporativa sin la autorización del Responsable de Seguridad Informática. En el caso de tratarse de usuarios que participen en un proyecto con tratamiento de información con Confidencialidad Reforzada, se podrán aplicar medidas de refuerzo de la seguridad a criterio del socio responsable del proyecto. En el caso de usuarios que

participen en proyectos donde se trate información de Máxima Confidencialidad, el software autorizado quedará restringido a aquel autorizado en el CCN.

- Copia de seguridad de los ordenadores personales - Es responsabilidad del propio profesional de MS realizar las correspondientes copias de seguridad. Para ello se proporciona una herramienta de replicación automática a todos los profesionales (DVR).
- Eliminación segura de la información: Los responsables de los proyectos (socios y directivos) deberán identificar los requerimientos de borrado de la información relacionada con un proyecto tras la finalización de la relación contractual con el cliente. En el caso de que el acuerdo con dicho cliente exija la eliminación segura de la información a la finalización del proyecto, deberán enviar una solicitud al Responsable de Seguridad Informática para la ejecución de dicha eliminación de manera trazable y utilizando herramientas y procedimientos autorizados. Este proceso será obligatorio para documentación y datos asociados a proyectos de Máxima Confidencialidad.
- Uso de dispositivos no corporativos como smartphones, tablets, herramientas de almacenamiento masivo de datos, etc.:
    - Cuando un profesional quiera utilizar dispositivos no corporativos deberá solicitar a Tecnología la autorización y en su caso instalación de una licencia corporativa de MDM/MAM con objeto de garantizar las normas de seguridad de la Firma (acceso seguro y confidencialidad de la información de la firma y de los clientes).
    - Si en algún momento se descarga o copia información en cualquier medio de almacenamiento contenido en el dispositivo (bien copiando, abriendo o descargando un documento), el profesional se asegurará de que el medio esté cifrado y de que la clave de desencriptación sólo es conocida por él. Además, deberá eliminar de forma inmediata la información cuanto dejen de estar vigentes los motivos que justificaron el almacenamiento temporal de dicha información.
    - En ningún caso se almacenarán credenciales en dispositivos no corporativos (ej: en el navegador)
- Las formas de acceso segura a los servicios corporativos desde diferentes dispositivos son las siguientes:
    - De forma directa (por cable o por la red inalámbrica corporativa) en la oficina de MS utilizando ordenadores corporativos.
    - Por VPN desde fuera de la oficina utilizando ordenadores corporativos y a través de WiFi o router MiFi.
    - Por interfaz web para el servicio de DVR desde fuera de la oficina. En el caso de acceder desde un dispositivo no corporativo se prohíbe explícitamente el almacenamiento de archivos y credenciales (ej: en el navegador).
    - A través del cliente MDM/MAM corporativo instalado en el dispositivo móvil corporativo o no, en el último caso previa solicitud y autorización de Tecnología en base a la política definida por MS.

Cualquier otra forma de acceso no está permitida.

Respecto a la reducción de la **huella digital**, se requiere que los profesionales:

- Configuren las opciones de navegación permitiendo solo los registros de navegación exclusivos para el buen funcionamiento de la web a la que acceden y se evite así dar información no deseada sobre el uso que hacemos de cada web.
- Adicionalmente, en el uso de dispositivos de escritorio y personales, se recomienda que:
  - Se comparta información en la nube o DVR de manera que se reduzca el número de copias de un mismo archivo.
  - Se eliminen los ficheros duplicados o con un número alto de versiones que no aporten valor.
  - Se eliminen fotos o videos repetidos o que no aporten valor al ámbito de trabajo para el que se utilizan los dispositivos.
  - En el uso del correo electrónico:
    - Reduzcan el número de destinatarios de los correos.
    - Eliminen correos que no sean de tu interés o bien contengan información obsoleta.
    - Se den de baja de newsletters que no sean de utilidad.
    - Vacíen regularmente la papelera

Todos los profesionales de MS y, cuando sea pertinente los usuarios externos y los terceros que desempeñen funciones en MS, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos MS por parte de la Dirección de Calidad y Auditoría Interna.

5.4. Auditorías y Monitorización de Uso

La Firma se reserva el derecho de realizar las auditorías que se consideren necesarias ante sospechas de incumplimiento de la presente política, monitorizando el uso que se esté dando a los recursos y a la información.

Por ello, todo empleado o proveedor con acceso a nuestros recursos, sistemas, o información, deberá ser consciente de que el uso que haga podrá ser monitorizado por la Firma. De esta forma, cada vez que se acceda al sistema, se mostrará el siguiente aviso:

"*De conformidad con la Política de Seguridad de Management Solutions, se recuerda la necesidad de utilizar los recursos tecnológicos proporcionados por la firma (ordenadores portátiles, teléfonos móviles, smartphones, equipos multifunción…), con la debida diligencia y para los fines exclusivamente relacionados con el desempeño de las actividades propias de la función y/o servicio de colaboración, pudiendo incurrir, en caso contrario, en la exigencia de responsabilidades legales. En este sentido, Management Solutions monitoriza y, ante sospechas de posibles vulneraciones de las normas de uso, valorará la necesidad de investigar los accesos y/o usos de los recursos informáticos por parte de los profesionales de la firma y/o colaboradores que utilizan equipos nuestros que representen una amenaza a la seguridad de los Sistemas de Información y/o pudieran causar perjuicios de cualquier otra índole a la firma. Para mayor información consulte las Políticas Corporativas.*"

Los ámbitos que se monitorizan sistemáticamente son los siguientes:

- Inventario de aplicaciones instaladas en cada equipo: Monitorización de consumos telefónicos (fijos y móviles)
- Monitorización del consumo del servicio de videoconferencia
- Navegación por internet:
- Monitorización de impresiones, copia y escaneo de documentos
- Registro de conexión a red y acceso remoto a través de VPN
- Registro de eventos del propio sistema operativo Windows
- Monitorización del correo electrónico (fecha, hora, asunto, emisor, receptor)
- Monitorización de la última conexión desde dispositivos corporativos o no con licencia corporativa MDM instalada e información básica del dispositivo (marca, modelo, versión sistema operativo, operador, etc…)

6. Logs proporcionados por Microsoft 365

TÉRMINOS Y DEFINICIONES

A efectos de una correcta interpretación del presente documento, se realizan las siguientes definiciones:

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de ordenador, audiovisual u otro.

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la información: Se refiere al hardware y software operados por MS o por un tercero que procese información en su nombre, para llevar a cabo una función propia de MS, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Seguridad de la información: La seguridad de la información se caracteriza por el cumplimiento de las siguientes características:

- Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, siempre que lo requieran, desde cualquier ubicación en la que se requiera (instalaciones MS, externas, ubicación geográfica mediante conexión por VPN, etc.)
- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto MS.
- Confiabilidad de la información: que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones según su naturaleza.

Evaluación de riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de MS. Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo de forma periódica.

Incidente de seguridad: Un incidente de seguridad es un evento adverso en el sistema de seguridad establecido que comprometa la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información.