



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

EXCEM GRUPO

INTRODUCCIÓN

Este documento desarrolla la política de seguridad de la información de EXCEM GRUPO, de obligado cumplimiento para todo el personal de EXCEM GRUPO y colaboradores.

CONFIDENCIALIDAD Y DEBER DE SECRETO

- Se considera información confidencial al conjunto de todos los datos personales tratados en los sistemas de información de EXCEM GRUPO, así como toda aquella información a la que se tenga acceso o se desarrolle como cumplimiento de las funciones y obligaciones que han sido asignadas por la organización para el desempeño del puesto de trabajo.
- Se debe proteger la información confidencial estableciendo medidas de control que garanticen e impidan el acceso no autorizado, incluyendo la simple visualización.
- Se debe reducir el uso de información confidencial a lo estrictamente necesario para la prestación de los servicios para los que ha sido contratado.
- Se debe mantener en todo momento el secreto profesional respecto a la información confidencial con la que se trata. Esta obligación persistirá por tiempo indefinido, aún después de finalizar sus relaciones profesionales con EXCEM GRUPO, devolviendo cualquier soporte o documento que contenga información confidencial.
- Queda prohibida la transferencia de información de carácter personal a terceros, por cualquier medio (en soporte papel, magnético, electrónico,...) excepto a las personas o entidades debidamente autorizadas por razón de su cargo o competencias dentro de EXCEM GRUPO por los responsables competentes.

NOTIFICACIÓN Y REGISTRO DE LAS INCIDENCIAS DE SEGURIDAD

- Se considerará incidencia de seguridad cualquier anomalía que pueda ser detectada en relación con la seguridad de la información.
- Es obligación de todo el personal comunicar cualquier incidencia de seguridad. Esta comunicación debe llevarse a cabo a través del Departamento de Informática (Tecnologías de la Información) y de forma inmediata a su conocimiento.

SOFTWARE CORPORATIVO Y EQUIPOS HOMOLOGADOS

- Se debe utilizar exclusivamente software autorizado por EXCEM GRUPO y equipos corporativos.
- El usuario no podrá realizar acciones u omisiones tendentes a provocar la desactivación de las medidas de seguridad implantadas en el soporte que EXCEM GRUPO le ha asignado. Para las excepciones a esta norma por motivos justificados, se requerirá autorización del responsable del departamento.
- En caso de que sea necesaria la instalación de software, el Departamento de Tecnologías de la Información será el responsable de realizar dicha instalación y supervisará que se realice de acuerdo a las políticas de seguridad de la empresa, que a su vez se ajustan a los protocolos y estándares de licenciamiento de software de Excem Grupo. En caso de que una instalación sea realizada por el empleado sin supervisión de IT, será necesario que éste haya obtenido una autorización por escrito para ello de su responsable de departamento. Este tipo de instalaciones deben estar sujetas así mismo a los protocolos establecidos en la empresa en materia de seguridad de la información y con arreglo a las condiciones legales de instalación y uso de dichos productos.
- Excem Grupo supervisará de manera activa y con regularidad el estado de las licencias de los equipos, pudiendo llegar a bloquear, aislar o llevar a cabo cualesquiera otras acciones que estime necesarias de forma preventiva si detectara la instalación de software no autorizado, además de proceder a la desinstalación de dicho software.

AUTORIZACIÓN DE ACCESO AL SISTEMA DE INFORMACIÓN

- Cada empleado con acceso a los sistemas de información de EXCEM GRUPO tiene asignado un identificador de usuario y una contraseña o certificado electrónico, de cuyo uso se responsabiliza personalmente.
- El identificador de usuario y su contraseña o certificado electrónico son de carácter personal e intransferible. El usuario tiene la obligación de notificar cualquier incidencia si sospecha que sus credenciales de autenticación han sido comprometidas.
- La contraseña deberá ser cambiada al menos cada 3 meses.
- La longitud mínima de la contraseña deberá ser de 7 caracteres y deberá contener caracteres alfabéticos, numéricos y signos de puntuación.
- Los usuarios no deben almacenar contraseñas o cualquier otra información de acceso en sistemas portátiles o remotos. Si se utilizan generadores de contraseñas dinámicos u otros mecanismos de control de acceso, éstos no deben almacenarse en el mismo lugar que los ordenadores portátiles.
- Se debe acceder exclusivamente a aquellos datos y recursos que se precisen para el desarrollo de las funciones encomendadas por EXCEM GRUPO.
- En caso de tener que almacenar generadores de contraseñas o mecanismos de control de acceso en equipos portátiles o remotos, estos sistemas deberán disponer a su vez de las pertinentes medidas de control de acceso para evitar su uso por parte de personal no autorizado.

CONTROL DE ACCESO FÍSICO

- Únicamente el personal autorizado por EXCEM GRUPO debe tener acceso a las áreas de acceso restringido.

GESTIÓN DE SOPORTES Y DOCUMENTOS

- El envío telemático y la salida de soportes y documentos que contengan datos de carácter personal, fuera de los locales bajo el control de EXCEM GRUPO, deberá ser autorizada a través del Departamento de Tecnologías de la Información. Para los datos de carácter personal de alto nivel, además se protegerá su envío con las herramientas de cifrado aprobadas por EXCEM GRUPO. Se consideran datos personales de nivel alto los referentes a ideología, religión, creencias, origen racial, salud, vida sexual y datos recabados para fines policiales.

GESTIÓN DE FICHEROS TEMPORALES, COPIAS DE TRABAJO DE DOCUMENTOS Y TRATAMIENTOS DE DATOS FUERA DE LAS INSTALACIONES

- Se consideran ficheros temporales aquellos archivos que se creen exclusivamente para la realización de trabajos temporales o auxiliares, mediante las extracciones totales o parciales de datos con información confidencial.
- Todo fichero temporal o copia de trabajo debe ser borrado o destruido una vez haya dejado de ser necesario para los fines que motivaron su creación.
- Debe evitarse siempre que sea posible almacenar información confidencial en unidades locales de los equipos de usuario o en soportes extraíbles. La información confidencial del usuario debe ser almacenada en su carpeta personal de red, así como en la carpeta de red de su departamento/área.
- La realización de copias o reproducción de los documentos con datos personales de nivel alto sólo se podrá llevar a cabo bajo la autorización del responsable competente y deberá solicitarse a través del Departamento de Tecnología de la Información. Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida.

USO APROPIADO DE LOS RECURSOS FÍSICOS Y LÓGICOS QUE TRATAN INFORMACIÓN CONFIDENCIAL.

- El sistema informático, los sistemas de archivo, la red corporativa y los terminales utilizados por cada usuario son propiedad de EXCEM GRUPO y su uso se limitará a las actividades y tareas directamente relacionadas con la actividad de la empresa y las funciones del puesto de trabajo del usuario.
- Cada equipo corporativo de EXCEM GRUPO estará asignado a un usuario o grupo de usuarios que deberá garantizar la guardia, custodia y el buen uso de este, impidiendo el acceso no autorizado al terminal.
- Los usuarios deben apagar el equipo al final de la jornada laboral o durante una ausencia prolongada. Si por algún motivo debe mantenerse encendido se debe bloquear mediante contraseña.

USO DEL CORREO ELECTRÓNICO Y EL ACCESO A INTERNET

- Los mensajes recibidos al correo electrónico de EXCEM GRUPO no serán considerados privados. Se considerará correo electrónico tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas.
- EXCEM GRUPO se reserva el derecho a revisar, sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la empresa como responsable civil subsidiario. La precitada comprobación de correos se realizará únicamente cuando se tengan fundadas sospechas de un uso indebido de las herramientas informáticas y, en todo caso, se hará, en presencia del propio trabajador o de un representante del mismo.
- EXCEM GRUPO se reserva el derecho a monitorizar y comprobar, de forma aleatoria sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa.