POLÍTICA DE USO ADECUADO DE LOS ACTIVOS DE INFORMACIÓN

CLASIFICACIÓN	INTERNO
ÁMBITO DE DIFUSIÓN	USUARIOS CON ACCESO A ACTIVOS DE INFORMACIÓN CORPORATIVA Y CANDIDATOS DE NUEVO INGRESO

ÍNDICE

1. OBJETO

El objeto de la presente política es definir las directrices que deben aplicarse para regular el uso que hacen los usuarios de los activos de información y de los datos personales que ESIC pone a su disposición para el desarrollo de sus funciones.

2. ALCANCE Y ÁMBITO DE APLICACIÓN

2.1. Ámbito objetivo

Esta política aplica a todas las actividades y procesos de negocio corporativos, en el ámbito de la gestión de la información, en su obtención, tratamiento y cesión de datos.

2.2. Ámbito subjetivo

El alcance subjetivo de este documento es transversal y de obligado cumplimiento por todo usuario con relación laboral, mercantil, académica o de cualquier otra naturaleza, que tenga acceso a activos de información de ESIC, tanto Business & Marketing School como University. Ello incluye a empresas externas que puedan asumir el rol de encargados de tratamiento de datos personales.

2.3. Ámbito material

Las presentes normas de seguridad son de aplicación a los recursos protegidos que dispone ESIC y los datos personales de los que es encargado de su tratamiento.

3. DIRECTRICES GENERALES

Los sistemas informáticos y la información que contienen, la red corporativa, el acceso a Internet, los dispositivos, los servicios y las credenciales de acceso proporcionados al usuario son propiedad de ESIC.

Las personas que trabajen, presten o reciban servicios de ESIC, deben preservar la seguridad de los activos que la compañía pone a su disposición, en consonancia con los criterios, requisitos, procedimientos y tecnologías de seguridad definidas en los Marcos Normativos ISO 27001 e ISO 27701 y las leyes aplicables en materia de seguridad y privacidad de la información (RGPD y LOPDGDD).

En el caso de empresas externas que asuman el rol de encargado de tratamiento de datos personales y con Empresas de Trabajo Temporal (ETT), ESIC establecerá en el contrato correspondiente la obligación de que el personal de las mismas, en su relación con ESIC, cumpla con las obligaciones de esta política.

El acceso a los medios y Sistemas de Información facilitados por la Organización se condicionan a estas obligaciones:

3.1. Conocer y cumplir la presente Política, así como las consecuencias de su incumplimiento, y cumplir con las obligaciones legales, estatutarias, reglamentarias y contractuales aplicables y, especialmente, con la legislación de protección de datos personales en vigor.

3.2. Limitar el uso de los medios facilitados por la organización a los temas directamente relacionados con la actividad de ESIC y las funciones del puesto de trabajo o servicio prestado, con el fin exclusivo de facilitar su actividad laboral, profesional o educativa y solo durante el tiempo que dure la relación. El uso adecuado de los activos proporcionados a los usuarios será objeto de comprobación y monitorización.

3.3. Acceder solamente a aquella información que sea estrictamente necesaria para desarrollar las tareas asignadas y guardar secreto profesional sobre los datos sensibles de los que se tenga conocimiento, durante y después de finalizar la relación laboral, mercantil o docente.

3.4. Poner en conocimiento del Responsable de Seguridad de la Información, ciso@esic.edu, o del Delegado de Protección de Datos, dpd@esic.edu, en caso de que se vean afectados datos de carácter personal, cualquier incidente, sospecha o duda que pueda afectar a la información corporativa o tratada de terceros.

3.5. Participar en las sesiones formativas en la materia a las que se convoque y superar las evaluaciones que evidencien la capacitación mínima exigible.

4. DIRECTRICES RELACIONADAS CON EL CONTROL DE ACCESO

ESIC asignará a cada usuario de los sistemas de información una identificación (cuenta y contraseña) para su acceso a los recursos corporativos, que serán asignados por la organización según la regla de mínimo privilegio de la Política de Control de Acceso Lógico. El usuario es el responsable de tratar de forma confidencial y custodiar adecuadamente las contraseñas que le sean proporcionadas a tal fin, evitando el acceso a las mismas de terceras personas y, en concreto, de cumplir con las siguientes reglas:

4.1. Mantener la confidencialidad de las credenciales de acceso y no compartirlas con nadie, incluido el personal de la propia entidad. En caso de incumplimiento de esta directriz, el usuario podrá ser responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada el identificador del usuario.

4.2. No está permitido la escritura, copia o reproducción de las credenciales en papel o en un documento electrónico sin protección (documento sin cifrar y/o almacenado en un volumen sin cifrar).

4.3. No utilizar las mismas credenciales en servicios externos (RRSS, banca personal, blogs, etc.) u otros propósitos ajenos a la organización.

4.4. Comunicar inmediatamente cualquier anomalía o incidente (robo, pérdida, etc.) que se tenga con las mismas.

4.5. Cambiar las contraseñas iniciales o reiniciadas en el primer acceso, cuando nos lo indique el sistema por su caducidad y siempre que se tenga sospecha de que han podido ser comprometidas.

4.6. Emplear siempre, aunque el sistema no lo fuerce, multifactor de autenticación y contraseñas que cumplan con la complejidad (Mayúsculas, minúsculas, números y símbolos), longitud (>10 caracteres) y caducidad (<180 dias) establecidas en la normativa.

4.7. Ante una baja o ausencia prolongada del usuario o tras el cese de la relación por baja definitiva, fin del ciclo formativo, despido o jubilación, las cuentas de acceso a todos los sistemas serán bloqueadas. En el caso de empleados, el Responsable del Departamento o Campus del usuario que causa baja, podrá solicitar al Responsable de Seguridad, a través del Service Desk, la redirección del correo o el acceso a esos sistemas o información con el objeto de continuar las actuaciones profesionales que correspondan, pero en ningún caso accediendo con la identidad del que causa baja. Cfr. 6.3.9

Los alumnos que finalicen su ciclo formativo y lo deseen, conservarán como alumni su identidad y cuenta de correo, pero no el resto de los servicios de M365.

5. DIRECTRICES RELACIONADAS CON EL PUESTO DE TRABAJO Y LOS DISPOSITIVOS

ESIC proveerá de los medios para poder ejercer las funciones que se asignen al usuario desde cualquier ubicación y dispositivo, pero puede poner a disposición del usuario diferentes recursos para su empleo exclusivo con fines profesionales o docentes y relacionados con su actividad en la organización, siendo responsabilidad del usuario su buen uso y el cumplimiento de las siguientes directrices:

5.1. Mesa limpia en el puesto de trabajo

El puesto de trabajo es donde se llevan a cabo las funciones profesionales o docentes, tanto dentro como fuera de las instalaciones de ESIC, y es responsabilidad del usuario mantenerlo despejado y controlado.

5.1.1. Guardar bajo llave la información sensible impresa en papel o almacenada en soportes digitales (discos externos, pendrives, etc.). Cfr. 5.2.12 y 7.1

5.1.2. No desatender la información en impresoras comunes.

5.1.3. No almacenar información personal y/o objetos de valor en los escritorios o espacios de la organización, ni información sensible fuera de espacios protegidos.

5.2. Uso de dispositivos

Los dispositivos proporcionados por ESIC son propiedad de la organización y el usuario debe cuidarlos y devolverlos en buen estado cuando se requiera o cuando acabe o suspenda la relación en caso de baja o de excedencia. El usuario deberá seguir las siguientes directrices:

5.2.1. Está prohibido modificar, salvo autorización previa, la configuración de seguridad que tenga cualquier dispositivo entregado por la organización.

5.2.2. Proteger y cuidar todos los dispositivos que la organización pone a su disposición, especialmente fuera de las instalaciones de la misma. Los daños o extravíos de los dispositivos por negligencia o reincidencia del usuario, excluyendo el lógico desgaste por el uso o por accidentes inevitables, podrá implicar sanciones compensatorias.

5.2.3. Utilizar los dispositivos con un bloqueo de pantalla, activado tras un periodo de inactividad y que necesite ser desbloqueado por contraseña, patrón o elementos biométricos.

5.2.4. Apagar de forma ordenada los dispositivos al finalizar la jornada laboral o lectiva.

5.2.5. Bloquear o cerrar la sesión de trabajo del dispositivo al ausentarse del puesto de trabajo, incluyendo recursos compartidos como aulas, salas de reuniones o despachos y, especialmente, en ubicaciones fuera de la Organización.

5.2.6. No desactivar ni desconfigurar los mecanismos de seguridad instalados en los dispositivos (gestión remota, cortafuegos personales, antivirus, etc.).

5.2.7. No intentar aumentar el nivel de privilegios de usuario en los dispositivos.

5.2.8. No borrar programas o ficheros que impidan o dificulten el normal funcionamiento del dispositivo.

5.2.9. Permitir las actualizaciones de seguridad, incluyendo la reinstalación completa del dispositivo, y de las firmas del antivirus, de acuerdo a las configuraciones y mecanismos establecidos por la organización,

5.2.10. Utilizar solo las herramientas de copia de seguridad de la organización para mantener el respaldo de la información.

5.2.11. Seguir los procedimientos de instalación y configuración de los sistemas y dispositivos facilitados por la organización, reportando de forma inmediata cualquier anomalía que se detecte en los mismos.

5.2.12. No utilizar equipos ni soportes de almacenamiento externos (papel, pendrives, discos…) para información corporativa sin autorización expresa, utilizando en su lugar las herramientas de la nube corporativa.

5.2.13. Si el dispositivo se extravía o se sospecha del acceso de persona no autorizada, se deberá comunicar de inmediato al responsable técnico para el cambio de contraseña y la aplicación de las medidas necesarias.

5.2.14. Devolver todos los dispositivos en perfecto estado, asumiéndose un desgaste normal por el uso, a la finalización de la relación con la Organización o cuando se solicite para su renovación o mantenimiento. En caso de proveedores y personal externo, la organización subcontratada será la encargada de exigir la devolución de los activos. Además, deberán borrar todas las copias electrónicas y destruir aquellos soportes no re-escribibles que las contuvieran, una vez que la información no sea necesaria para el cumplimiento del contrato.

5.3. Dispositivos móviles y Teletrabajo

En el caso de emplear dispositivos móviles corporativos (portátiles, teléfonos,…) fuera de las instalaciones de ESIC, se deben cumplir, adicionalmente, con las siguientes obligaciones, incluidas en la Normativa de Teletrabajo y Dispositivos Móviles.

5.3.1. Extremar las precauciones en el transporte de estos dispositivos y cuidarlos adecuadamente

5.3.2. Asegurarse de que no hay nadie observando la información mostrada en la pantalla del dispositivo, especialmente en sitios públicos, transportes, cafeterías, hoteles o similares. Utilizar filtros de privacidad si es preciso

5.3.3. Asegurarse de que emplea conexiones a Internet seguras, utilizando la VPN corporativa y contraseña robusta en la conexión a la Wifi doméstica, priorizando la conexión cableada y celular frente a la Wifi, y evitando los puntos de acceso Wifi públicos o sospechosos.

5.3.4. Mantener la aplicación de MDM (Mobile Device Management) instalada en el dispositivo y aceptar el acceso, geolocalización o bloqueo por parte del personal técnico autorizado de la organización.

5.3.5. Evitar el uso por terceros del dispositivo, incluidos familiares directos.

5.3.6. Mantener el cifrado del dispositivo móvil según se entrega por el departamento técnico

5.3.7. Antes de desplazamientos profesionales al extranjero, notificarlo por ServiceDesk al servicio técnico para prepararlo (roaming, VPN, etc.)

5.4. Uso de dispositivos no corporativos

En general, no se deben utilizar dispositivos no controlados por la organización para funciones profesionales, especialmente si trata datos sensibles o de carácter personal.

En el caso de no disponer de equipo corporativo o que se precise hacer uso de uno no controlado por ESIC para fines profesionales o docentes, se deben cumplir las siguientes directrices, adicionales a todas las anteriores que apliquen:

5.4.1. En el caso de personal con equipo corporativo, debe ponerlo en conocimiento del Responsable de Seguridad y ser autorizado para ello.

5.4.2. No utilizar la línea (SIM) corporativa en dispositivos particulares, ni viceversa, sin autorización.

5.4.3. Utilizar una cuenta exclusiva de bajos privilegios (invitado) del sistema operativo para uso profesional o docente, diferente de la personal (habitualmente de privilegios de administrador).

5.4.4. Utilizar autenticación de acceso de suficiente seguridad (biométrico o contraseña compleja y no permanente) y preferentemente con multifactor.

5.4.5. Finalizar las sesiones de usuario abiertas en los dispositivos cuando no las necesite y eliminar los archivos temporales, descargas, historial de

navegación, contraseñas y cookies, utilizando el modo privado en los navegadores (‘Incognito’ o ‘InPrivate’)

5.4.6. Actualizar las aplicaciones facilitadas por la Organización y conocer su manejo de forma segura según las indicaciones del personal de soporte y mantener actualizado el Sistema Operativo y las firmas del antivirus.

5.4.7. Evitar la descarga de archivos y adjuntos de correos para que no se almacenen copias no cifradas de información sensible en el dispositivo.

5.4.8. En el caso de que el dispositivo particular sea portátil se deberá disponer de herramientas para la encriptación de los datos confidenciales.

5.4.9. En el caso de que el dispositivo se encuentre involucrado en un incidente de ciberseguridad dentro de ESIC, puede ser retenido como evidencia.

5.4.10. Evitar la instalación de software y descarga de ficheros desde fuentes sospechosas

5.4.11. Evitar el uso de VPN gratuitas o de baja reputación, pues la detección de accesos desde ubicaciones o IP sospechosas podrán bloquearse.

6. DIRECTRICES RELACIONADAS CON EL USO DE APLICACIONES

Las aplicaciones necesarias para las funciones del usuario están preinstaladas en el dispositivo que se entrega o son accesibles con las credenciales proporcionadas. Si se precisa de alguna más específica, debe solicitarse a soporte técnico, con la aprobación del responsable del usuario, del CTO y el CISO, a través del Service Desk.

6.1. En general

6.1.1. Utilizar únicamente software homologado, instalado y licenciado por la organización, cumpliendo con la normativa de propiedad intelectual o industrial del software, quedando expresamente prohibido instalar copias ilegales de cualquier programa y/o borrar cualquiera de los programas instalados legalmente en los equipos corporativos

6.1.2. No se deberán utilizar servicios particulares o no autorizados para fines profesionales o académicos (correo personal, WeTransfer, Dropbox, Facebook, WhatsApp…), especialmente aquellos usos en los que intervengan datos confidenciales o de carácter personal. Recíprocamente, no deberán utilizarse sin autorización recursos ni servicios de ESIC para fines particulares (correo corporativo, almacenamiento, PC, teléfono…)

6.1.3. No introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros

6.1.4. Acceder a los datos y editarlos preferentemente a través de las aplicaciones ofimáticas online, la mayoría integradas en M365.

6.2. Uso de la web

6.2.1. Abstenerse de acceder a páginas web con contenido malicioso, pornográfico o ilegal y, en general, para fines no profesionales o docentes.

6.3. Uso del correo

6.3.1. Debe limitarse el uso del correo solo para comunicaciones con contactos externos (clientes, proveedores…), priorizando la utilización de Teams para la comunicación interna y Canvas para la académica.

6.3.2. No se deberán reenviar correos corporativos a cuentas personales, ni viceversa, sin autorización expresa.

6.3.3. Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios sin autorización.

6.3.4. Se optará preferentemente por el acceso web, https://mail.esic.edu, en lugar de clientes de correo (Outlook) que mantienen información en el dispositivo, y siempre que se acceda desde equipos no corporativos.

6.3.5. Se limitará el número de destinatarios de correo, pudiéndose ampliar por causa justificada, debiéndose emplear los medios adecuados proporcionados por la Organización para envíos masivos.

6.3.6. Ante un correo sospechoso deberá evitarse interactuar con él: responder, abrir cualquier fichero adjunto o hacer clic en cualquier enlace y comunicarlo de inmediato al soporte técnico de la organización a través del ServiceDesk.

6.3.7. Utilizar la copia oculta (CCO) cuando se envíen mensajes a numerosos destinatarios, especialmente si alguno de ellos es de fuera de la organización, y comprobar que los destinatarios son correctos.

6.3.8. Está terminantemente prohibido enviar mensajes de correo electrónico, a o desde buzones corporativos, hirientes, calumniosos, injuriosos o que puedan producir cualquier perjuicio a ESIC o a sus destinatarios, o enviarlos con fines comerciales o publicitarios sin el consentimiento del destinatario y del DPD. Bajo ningún concepto se utilizarán servicios externos de envío de correo como Mailchimp o similares no autorizados.

6.3.9. Está prohibido el acceso a cuentas de correos de otros usuarios, excepto en caso de su baja definitiva y en los supuestos establecidos.

Para el personal laboral y en los casos de vacaciones, permisos, ausencias prolongadas, bajas por enfermedad y situaciones análogas, los mensajes de correo podrán ser redirigidos a su superior jerárquico u otra persona de su equipo para poder continuar con la actividad profesional.
Para acceder al buzón de correo de un usuario será preciso que su responsable y el CISO o DPD lo autorice. En cualquier caso, solamente se accederá para consultar información y nunca para enviar correos, pudiendo convertir el buzón del que causa baja en compartido y agregando al sustituto que asigne el responsable, previa autorización del CISO o DPD.

6.4. Uso de M365

M365 y sus herramientas incluidas (Teams, Onedrive, Sharepoint, Planner, Office…) constituye el entorno de trabajo colaborativo corporativo. El uso de cualquier otra aplicación para fines profesionales o docentes debe estar previamente aprobada por la Unidad de Innovación Digital (UID) y el responsable de seguridad o el DPD.

6.4.1. Todos los Grupos y Equipos (Teams) deben ser creados por el departamento de sistemas de UID, asignando como propietario del mismo al responsable del área o departamento solicitante, siendo este el encargado de asignar los miembros y sus derechos.

6.4.2. Los usuarios externos (colaboradores, proveedores, auditores…) podrán incluirse como invitados del dominio con su cuenta externa o, si excepcionalmente se precisa que sean miembros del dominio, se le podrá generar una cuenta temporal del tipo usuario@externo.esic.edu. En ambos casos, debe solicitarlo el responsable del solicitante y aprobarlo el CISO a través del Servicedesk, verificando el compromiso de confidencialidad (NDA) o contrato de encargado de tratamiento de datos personales (CET) para las entidades jurídicas y el conocimiento de la presente Política para las personas físicas.

6.4.3. El uso del entorno se restringe a fines profesionales y docentes, exclusivamente mientras dure la relación laboral o mercantil y según las reglas de “etiqueta” ya indicadas en el punto 6.3.8, para Chats, Publicaciones, etc.

6.4.4. No deberá extraerse o compartir información interna fuera del entorno M365, especialmente si es confidencial o contiene datos de carácter personal sin autorización previa del DPD.

6.4.5. Los derechos de acceso a los recursos a través de vínculos en M365, deberán de restringirse a los usuarios y privilegios estrictamente necesarios.

6.4.6. No deberán sincronizarse carpetas o archivos de Sharepoint (Teams o OneDrive), especialmente si el dispositivo no está cifrado y en ningún caso si además el equipo no es corporativo.

6.4.7. No se podrá acceder al OneDrive de otro usuario salvo en caso de su baja definitiva y en los supuestos establecidos, análogamente al punto 6.3.9,

6.5. Uso de otras aplicaciones en la nube

6.5.1. No se extraerá información de los sistemas de información corporativos en la nube (CRM, ERP…) sin autorización del DPD

6.5.2. No se utilizarán herramientas web no autorizadas para tratar información corporativa sensible (conversores de formato [PDF], asistentes de IA generativa, transferencia de ficheros, etc.)

7. DIRECTRICES RELACIONADAS CON EL TRATAMIENTO DE INFORMACIÓN

La información corporativa es uno de los principales activos de la Organización y su protección es el fin último de la Seguridad y Privacidad, por lo que se deberán cumplir las siguientes directrices sobre su tratamiento:

7.1. Trabajar siempre con archivos electrónicos en el entorno cloud corporativo y no redundarlos en otros soportes físicos o digitales sin autorización.

7.2. Seguir las **normas sobre clasificación y tratamiento de la información** definidas por la organización (Ref. C), especialmente en lo que respecta al etiquetado, inventariado y custodia de la información sensible.

7.3. Preservar la confidencialidad de la información en conversaciones, confirmando que nos son escuchadas o grabadas por terceros no autorizados e informando a los presentes de su sensibilidad al inicio de estas.

7.4. Proteger la información que comparte con organizaciones externas según los criterios, requisitos, procedimientos y tecnologías de seguridad definidos por la organización.

7.5. No publicar ni almacenar sin autorización información de la organización (documentos, vídeos, opiniones, etc.) en servidores públicos de Internet (blogs, servicios de almacenamiento, repositorio de ficheros, vídeos, correo no corporativo, clientes de mensajería no corporativos, redes sociales, etc.).

7.6. No mantener en local los ficheros con la sincronización SharePoint / OneDrive ni almacenar datos sensibles en dispositivos personales ni corporativos

7.7. Cualquier información introducida en la red corporativa a través de cualquier vía debe cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial, privacidad y a control de virus y demás códigos maliciosos.

7.8. Los usuarios de los sistemas de información corporativos deben guardar la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o entidades, los datos, listas de correo, listas de empleados, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación con ESIC y entidades relacionadas, tanto en soporte físico como electrónico o de forma verbal. Esta obligación continuará vigente tras la extinción del contrato, hasta que la citada información deje de ser confidencial o pase a dominio público.

7.9. En el caso de que el usuario entre en posesión de información confidencial bajo cualquier tipo de soporte, debe entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello determine derecho alguno de posesión, titularidad, copia o cobro de la referida información. Asimismo, el usuario debe devolver dichos materiales a la entidad, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación contractual.

7.10. Cualquier fichero ubicado en cualquier almacenamiento propiedad de ESIC, no generado por la actividad profesional o docente, especialmente con información de carácter personal, sospechosos de malware o de infringir derechos de autor, será bloqueado o eliminado notificándoselo al usuario y registrando la incidencia correspondiente**.**

7.11. Todo usuario que pretenda realizar una copia a otro soporte o ubicación, incluyendo los dispositivos corporativos, de cualquier información confidencial o susceptible de contener datos de carácter personal debe solicitar previamente autorización al Delegado de Protección de Datos, debiendo notificar los datos que contiene y la finalidad de la misma.

7.12. Destruir la información sensible cuando ya no sea necesaria, mediante el uso de destructoras, de seguridad al menos P-3 (200 fragmentos por A4), para información en soporte físico, utilizando herramientas de borrado seguro para información digitalizada y borrando las pizarras analógicas tras su uso.

Queda expresamente prohibido:

7.13. Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la Entidad o de terceros sin autorización.

7.14. Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la entidad, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

7.15. Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de ESIC o de terceros.

7.16. Introducir, descargar de Internet, reproducir, utilizar o distribuir cualquier tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.

7.17. Utilizar recursos telemáticos de ESIC, incluido Internet, de forma inadecuada a las actividades relacionadas con las funciones del usuario.

7.18. Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la entidad, en la red corporativa.

7.19. Extraer o compartir información fuera del ecosistema corporativo, especialmente si contiene datos de carácter personal, sin autorización previa

7.20. Enviar información confidencial, secretos empresariales o información valiosa que no deba compartirse de ESIC a terceros mediante soportes materiales o a través de cualquier medio de comunicación (verbal, SMS, correo, RRSS, APPs…), incluyendo la simple visualización o acceso, sin autorización previa del CISO y/o del DPD. Se considerará terceros cualquier usuario, servicio o dispositivo externo a la red corporativa (cloud pública y privada) de ESIC.

7.21. Realizar acciones comerciales o cualquier comunicación corporativa a personas físicas externas a ESIC a través de medios o bases de datos no autorizados**.**

8. PROCESO DISCIPLINARIO

El incumplimiento de esta normativa por parte de usuarios de ESIC, puede dar lugar a la apertura de expedientes disciplinarios y, en su consecuencia, la aplicación de las medidas legales o convencionales que correspondan.

En el caso de usuarios externos o que pertenezcan a otras organizaciones, puede implicar la rescisión, cancelación o finalización del contrato correspondiente con la organización prestadora del servicio.

Cuando existan indicios de uso ilícito o abusivo por parte de un usuario, la organización realizará las comprobaciones oportunas y, si fuera preciso, realizará una auditoría en los sistemas de información (incluyendo los dispositivos facilitados por la organización) utilizados por el usuario o a los que haya tenido acceso.

Los resultados de esta investigación podrán dar lugar a la interposición de las acciones legales que correspondan, en defensa de los derechos e intereses de ESIC, considerando la gravedad, el impacto, la intencionalidad y la reincidencia de los actos cometidos.