POLITICA DE SEGURIDAD DE IT ORPEA IBERICA Y FILIALES (en adelante "ORPEA Ibérica"

1. Política

Los sistemas y medios informáticos de ORPEA tienen la finalidad de contribuir al funcionamiento eficiente de ORPEA Ibérica; el personal propietario y usuario de dichos sistemas es responsable de la seguridad de los mismos.

2. Aplicación

La presente política es de aplicación a todo el personal usuario de los servicios y sistemas IT de ORPEA ibérica. Los servicios y sistemas afectados por esta política no necesariamente han sido suministrados por ORPEA ni son de su propiedad. No excluye a ningún empleado o empleado, contratista/asesor, proveedor de IT, suministrador, ni cliente.

3. Definiciones

ORPEA Ibérica: Es la sociedad cabecera de grupo ORPEA en España. A efectos del presente documento se considera también ORPEA Ibérica todas sus filiales o sociedades controladas (Atirual Inmobiliaria y DinmORPEA).

Propietario/a del sistema: Empleado/a con cargo directivo o responsable de departamento que está a cargo de los datos que contiene un sistema y del uso adecuado del mismo. Por lo general, esta persona o su superior no pertenecen al departamento de IT.

Manager IT: Persona con responsabilidad general sobre los servicios de IT de todo ORPEAIbérica.

Virus informático: Software no autorizado y generalmente malintencionado que se replica y se propaga a diversos medios informáticos y/o por una red. Puede provocar que el PC efectúe funciones no autorizadas (p. ej. apagarse, interrumpir el acceso a Internet, dañar ficheros, etc.).

Spamming: Envío de mensajes no solicitados, por lo general a clientes potenciales.

Spoofing: Envío de correo electrónico ocultando la dirección del remitente original.

Servicios críticos: Software o datos necesarios para garantizar la continuidad del negocio.

4. Directrices

El objeto de la seguridad de la información es garantizar la continuidad del negocio y minimizar los daños a la empresa, evitando o minimizando el impacto de incidentes relacionados con la seguridad.

La gestión de la seguridad en la información permite compartir información al tiempo que se asegura la protección de la información y de los activos informáticos. Se compone de tres elementos básicos:

a) Confidencialidad: impedir que una información delicada sea divulgada sin autorización o interceptada de forma inteligible.
b) Integridad: proteger la precisión y la integridad de la información, así como del software.
c) Disponibilidad: garantizar que la información y los servicios críticos estén disponibles para la persona usuaria cuando así se requiera.

La información puede adoptar muchas formas. Se puede almacenar en ordenadores, transferir a través de redes, imprimir, escribir o transmitirse de forma verbal. Desde el punto de vista de la seguridad, todas las formas de información se deben proteger de forma adecuada.

4.1. General

Todos los sistemas y medios informáticos y de información suministrados por ORPEA se han previsto para fines empresariales. Todos los programas, archivos o datos creados por un usuario en el entorno laboral destinado a fines empresariales pertenecerán siempre a la Empresa. El usuario se compromete a respetar los derechos de propiedad intelectual.

Queda estrictamente prohibido el uso de memorias o discos externos (USB) sin previa autorización.

Queda estrictamente prohibido el uso de cualesquiera de los sistemas informáticos o de información suministrados por ORPEA para violar la ley o que constituya parte de un acto ilegal.

Queda estrictamente prohibido el uso de cualesquiera de los sistemas informáticos o de información suministrados por ORPEA con el fin de acceder, descargar, transmitir o almacenar contenidos racistas, sexistas, ofensivos, o de carácter provocador explícito o similar.

Los sistemas informáticos de ORPEA no son para uso personal y deben utilizarse en consecuencia. ORPEA se reserva el derecho de supervisar y/o interceptar archivos o comunicaciones en cualesquiera de sus sistemas informáticos o de información, sin previo aviso a su autor, remitente o destinatario previsto.

Este seguimiento puede incluir, sin limitarse a ello, lo siguiente: lectura de correos electrónicos y archivos, registro y auditoría de acciones efectuadas y archivos consultados por los usuarios, bloqueo de la distribución de archivos y recuperación de datos de copias almacenadas.

Cuando un usuario o una usuaria del sistema no pueda acceder a la información (p. ej. enfermedad, vacaciones, viaje al extranjero, etc.), el responsable del usuario tendrá derecho sobre las carpetas del mismo para garantizar la continuidad del negocio. En caso de imposibilidad de acceso a las carpetas, el usuario acepta y consiente el cambio de su clave de acceso a fin de acceder a la información con el objetivo de dar continuidad al negocio. La Empresa siempre notificara al usuario de este acceso y esta acción está estrictamente supeditada a la aprobación de un directivo de ORPEA.

El uso de los sistemas y medios informáticos y de información de ORPEA por parte de una persona es un privilegio y no un derecho, y, como tal, puede ser retirado sin previo aviso en caso de abuso o incumplimiento de la ley por parte de esa.

4.2. Responsabilidad

La seguridad de un sistema de información es responsabilidad del propietario o propietaria del sistema. En materia de seguridad, los propietarios o propietarias de sistemas de información pueden delegar su autoridad en el personal encargado de los usuarios o usuarias. No obstante, continuarán siendo los responsables últimos de velar por la seguridad del sistema informático.

4.3.Formación

El personal usuario recibirá la formación pertinente en políticas y procedimientos de la organización, incluyendo los requisitos de seguridad y demás controles empresariales, así como formación sobre el uso correcto de equipos de IT antes de autorizar el acceso a los servicios IT.

4.4.Notificaciones

Los incidentes relacionados con la seguridad deben notificarse al Manager de IT (o, en su ausencia, a un miembro de la gestión de IT), lo antes posible y en todo caso de modo inmediato en caso de incidentes graves (por ejemplo, robo o sustracción de equipos o información).

Se considera incidente informático relacionado con la seguridad cualquier acontecimiento que dañe o amenace con dañar, ya sea de manera física o lógica, la seguridad de los sistemas y/o datos informáticos deORPEA. Esto incluye también la violación de los términos de la presente política de seguridad. Algunosejemplos son:

- El robo de equipos informáticos;
- La recepción de correo electrónico “inadecuado”
- El uso personal inadmisible de sistemas informáticos de ORPEA; y
- El robo de datos.

Esto no es una lista exhaustiva. Cualquier aclaración que se pueda requerir debería ser resuelta, con antelación, por el Manager de IT o un miembro del equipo de sistemas.

4.5.Control de acceso

Los usuarios y usuarias recibirán una ID de usuario y una contraseña únicas para cada uno de los sistemas a los que deban acceder. Las contraseñas son personales y confidenciales y queda terminantemente prohibido dar a conocer las mismas a terceros. Será responsabilidad del personal usuario asegurarse de que las contraseñas que se les proporcionen no se den a conocer públicamente o a terceros. Una vez haya accedido a un sistema seguro, el personal usuario no podrá dejar el sistema desatendido sin que se requiera una contraseña para poder acceder al mismo.

Aquellos usuarios y usuarias que tengan la sospecha de que alguien conoce sus contraseñas, deberán informar de tal situación al soporte de IT y cambiarlas inmediatamente.

Sera responsabilidad del superior/a de personal usuario que deje de trabajar con ORPEA comunicar la baja de éste al soporte de IT dentro de las 24 horas siguientes a la misma, de modo que se puedan anular el acceso al sistema y las contraseñas del usuario/a. Cuándo se tenga conocimiento de la baja de un usuario con antelación, deberá comunicarse de forma anticipada.

IT procederá al cierre definitivo de la cuenta del mismo en el plazo máximo de 72 horas desde que se produjo la baja.

El Soporte de IT no dará su consentimiento a que se compartan contraseñas allí donde los estándares empresariales o políticas de ORPEA, o bien la normativa o la legislación pertinente, requieran que la tarea especificada sea desempeñada únicamente por una persona identificada y autorizada.

IT deberá haber autorizado todos los dispositivos que se conecten a la red de ORPEA. [Incluso aunque la conexión sea únicamente para cargar el dispositivo]

Los dispositivos (PC, servidor, móvil, etc.) conectados a la red de ORPEA no pueden abrirse físicamente ni añadirse o retirar complementos/periféricos sin el previo consentimiento del departamento de IT.

En ningún caso, los dispositivos (PC, servidor, etc.) físicamente conectados a la red de ORPEA podrán estar simultáneamente conectados a otra red mediante módem, salvo si se cuenta con el consentimiento previo del departamento de IT.

El acceso remoto de terceras organizaciones tan solo estará permitido si cuentan con la autorización previa del departamento de IT deORPEA. Tal acceso deberá ser supervisado con el fin de dejar constancia de que todas las actividades efectuadas por la tercera parte queden, como mínimo, registradas e, idealmente, que también puedan ser verificadas de modo visual (mediante una observación de la actividad en tiempo real).

El acceso temporal o definitivo a cualquier carpeta, archivo, unidad de red, aplicación o servidor para un usuario o grupos de usuarios deberá ser previamente autorizado por el Responsable del área a que se refieren los mismos o por el Propietario del Sistema.

4.6. Control de virus

La amenaza de los virus informáticos está muy extendida y todo el personal usuario debe estar especialmente sensibilizado y concienciado de los daños potenciales que pueden generar los virus.

La empresa contribuye al control de virus adoptando las siguientes medidas:

- Se exige la observación de las licencias de software y se prohíbe el uso de software no autorizado.
- Se ejecuta software antivirus con una frecuencia definida para comprobar si los ordenadores y medios presentan alguno de los virus conocidos.
- Se revisan con regularidad el software y el contenido de datos de los sistemas y se investiga la existencia de archivos falsos o modificaciones no autorizadas.
- Se deben someter a un análisis de virus todos los medios extraíbles (discos, CD, lápices de memoria, etc.) antes de utilizarlos.
- Se debe informar de inmediato al soporte de IT de cualquier ataque de virus.
- Se deberán tratar siempre como sospechosos los datos adjuntos e hiperenlaces, de cualquier naturaleza, de un correo electrónico.
- Se debe eliminar el correo sin abrir los datos adjuntos o el enlace, siempre que llegue un correo electrónico de parte de alguien a quien no se conoce.
- Se debe llamar al remitente de un correo electrónico para confirmar el contenido de los datos adjuntos/enlaces antes de abrirlo, cuando éste nos llegue de un contacto profesional que habitualmente no envía datos adjuntos/enlaces o de quien no se esperaban datos adjunto/enlaces.

El departamento de IT contribuye a todas estas medidas para minimizar el riesgo de introducir un virus:

- Configurando software antivirus para escanear los archivos cuando se abran o graben y cuando entren o salgan correos electrónicos de ORPEA;
- Utilizando la tecnología adecuada para garantizar que se efectúan todas las verificaciones de virus necesarias, en todos los archivos que se descargan de Internet;
- Escaneando todos los equipos de IT que contienen medios informáticos devueltos o suministrados por terceras partes o proveedores (incluidos equipos en préstamo), antes de utilizarlos;
- No autorizando la conexión, ni el uso continuado en la red de ORPEA de equipos informáticos o software, ajenos a la empresa o que no se ajusten a los estándares, salvo si éstos satisfacen los requisitos de antivirus de ORPEA, en todo momento.

Los usuarios y usuarias deben saber que el departamento de IT se reserva el derecho de interrumpir la conexión a la red de ORPEA en cualquier momento, como parte de las acciones de protección contra virus.

Si un usuarioo usuaria no está seguro de que el software de antivirus instalado en su ordenador funcione correctamente, deberá contactar con el soporte de IT inmediatamente.

4.7. Correo electrónico

Se prohíbe el spamming.

El correo electrónico no puede ser difundido en redes sociales no profesionales o sitios web que no estén relacionados con el ámbito profesional.

En ningún caso, las personas usuarias podrán configurar sus sistemas de correo electrónico para que reenvíen automáticamente correos a destinatarios externos a ORPEA (incluidas sus cuentas personales externas a ORPEA).

Cuando ORPEA sea parte de un proceso de litigio, los usuarios y usuarias no deben eliminar bajo ninguna circunstancia ningún correo electrónico, si éste tiene que ver con el asunto en litigio. Si el personal usuario tuviera alguna duda sobre la relevancia de un correo electrónico en tal litigio, no deberán eliminarlo e informarán a su responsable del mismo.

El personal usuario no hará ningún intento de spoofing (según la definición anterior) ni de alterar la línea "De" u otra información relativa al origen de un mensaje.

Los correos electrónicos dirigidos o enviados por abogados y/o asesores en representación de ORPEA deberán incorporar la siguiente cabecera en todas las páginas: "SECRETO PROFESIONAL; NO REENVIAR SIN AUTORIZACIÓN."

Además de lo anterior, el personal usuario se asegurarádе incluir el pie firma, con el texto legal autorizado relativo a confidencialidad, cuando remita un mail a un destinatario externo.

4.8. Software

Se pone especial cuidado en el cumplimiento de las restricciones legales relativas al uso de materiales sujetos a copyright.

Cualquier tipo de software desarrollado por ORPEA será de propiedad exclusiva de ORPEAy no se podrá copiar ni emplear fuera de la empresa sin autorización.

El software de propiedad obtenido en virtud de un acuerdo de licencia, solo podrá emplearse ajustándose a las limitaciones definidas en la misma.

Las prohibiciones incluyen, aunque no se limitan a ello:

- Instalar o utilizar software o documentación relacionada, que no haya sido facilitada a ORPEA en virtud de una licencia, en los ordenadores o dispositivos de ORPEA.
- Copiar o distribuir software o documentación relacionada sin autorización o la licencia del propietario del copyright.
- Incumplir total o parcialmente los términos y condiciones de licencia o adquisición exigidos por los proveedores y que regulan el uso de software.

La violación del copyright puede causar que se emprendan acciones legales y, por este motivo, se efectuarán regularmente auditorías de software y se actualizarán los registros de software. Si en un ordenador se detectara la presencia de software que no aparece en el registro de licencias, éste será eliminado salvo que se puedan

obtener los discos originales y/o licencias. Si no se pudieran localizar los discos originales y/o licencias, se deberá volver a adquirir el software.

Asimismo, el personal tiene la responsabilidad de garantizar que no se violen las leyes de copyright y de licencia cuando redacten o reenvíen correos electrónicos o datos adjuntos.

En todo caso, la responsabilidad legal derivada del incumplimiento de lo anterior recae en el usuario o usuaria que contravenga esta instrucción.

El personal de IT es el único de ORPEA autorizado para instalar y configurar software en los ordenadores y dispositivos de la empresa. El departamento de IT debería comprobar la compatibilidad del software con los sistemas en uso en ORPEA y someter su instalación a los procesos habituales de control de cambios.

El departamento de IT se encargará de gestionar un registro actualizado de todos los activos de IT y de software autorizado a fin de que se pueda constatar el nivel de licencias vigentes en cada momento. Todo el software adquirido por ORPEA deberá quedar registrado en el departamento de IT. Además, los discos y licencias físicos deberán conservarse en una biblioteca de software.

4.9. Continuidad del negocio

Se revisará un plan de continuidad del negocio centrado en la preservación de los procesos y servicios empresariales esenciales que deben activarse tras el fallo, o deterioro, de equipos vitales. El proceso de planificación identificará y reducirá el riesgo de amenazas deliberadas o accidentales a servicios básicos y consistirá en:

- Identificar y priorizar los procesos empresariales fundamentales;
- Identificar y acordar todas las responsabilidades; y
- Documentar los procesos acordados.

El plan de continuidad del negocio está íntegramente recogido en un documento aparte.

4.10. Protección de losregistros

Se debe proteger los archivos importantes ante una posible pérdida, destrucción o falsificación. Puede ocurrir que algunos archivos deban preservarse, con el fin de satisfacer requisitos legales y respaldar actividades empresariales básicas.

A diario, se copiarán todos los datos inestables almacenados de forma centralizada. Se harán copias de los ficheros clave, siguiendo un patrón de intervalos especificado y éstos se conservarán durante un período de tiempo especificado.

Aquellos datos que se hayan grabado localmente en el disco duro de un PC (unidad “C:”) NO se copiarán, por norma, por lo que para evitar la pérdida de información se prohíbe el uso en local del ordenador “C:/”. Es responsabilidad de cada individuo asegurarse de que todos los datos que se deban copiar, se almacenen en una unidad de red (Citrix).

Las copias de generación múltiple de los datos clave se retendrán en una ubicación segura.

4.11. Equipos de IT

El departamento de IT aplicará procedimientos de suministro de IT para los equipos informáticos que:

- Establecen controles y modalidades que cubran la adquisición y/o el leasing dehardware y de software.
- Adquirirá única y exclusivamente equipos informáticos que satisfagan los estándares de ORPEA.

Todos los equipos informáticos proporcionados para ser utilizados dentro de ORPEA deberán ser aprobados por el departamento de IT.

IT aplicará procedimientos de eliminación de equipos que garanticen que todos los archivos y software se borran de forma definitiva de los discos duros, antes de ser devueltos al concluir un período de leasing, o antes de su eliminación. La venta/eliminación de equipos informáticos de ORPEA debe seguir al procedimiento de eliminación de IT.

Queda bajo la responsabilidad del personal usuario de equipos informáticos de ORPEA, comprobar que el material está seguro y que se utiliza adecuadamente. A continuación, se muestran algunos ejemplos de tratamiento inadecuado de equipos informáticos:

- Dejar ordenadores portátiles en lugares en los que corran un alto riesgo de ser robados, dañados o quedar expuestos a temperaturas excesivamente elevadas.
- Facturar ordenadores portátiles como si fueran equipaje ordinario, en lugar de como equipaje de mano.

Esto, no es una lista exhaustiva. Cualquier aclaración que se pueda requerir, debería ser resuelta con antelación por el Manager de IT o un miembro del equipo de sistemas.

No se permite al personal usuario definir o utilizar derechos de administrador en un PC u ordenador portátil, salvo cuando lo solicite el departamento de IT.

4.12. Cumplimiento de la política de seguridad

Todas las secciones de la organización serán sometidas regularmente a una revisión, con el fin garantizar el cumplimiento de la política y los estándares de seguridad.

Queda estrictamente prohibido cualquier intento deliberado de desactivar o sortear alguno de los sistemas de protección o supervisión de la red deORPEA, sin la autorización previa del Manager de IT.

El incumplimiento de esta Política de seguridad conllevará las acciones que legalmente correspondan a fin de derivar la responsabilidad a la personal incumplidora, reservándose ORPEA el ejercicio de las acciones legales que procedan para exigir responsabilidad y/o daños y perjuicios a la persona incumplidora.

4.13. Privacidad

Los sistemas informáticos y de correo electrónico de ORPEA pertenecen a la empresa y únicamente pueden emplearse con fines autorizados. Los empleados y empleadas pueden solicitar la lectura o el acceso a cualquiera de sus correos electrónicos, archivos u otros registros informáticos, creados por ellos o recibidos a su atención, almacenados en los sistemas informáticos o de correo electrónico de ORPEAen cualquier momento.

ORPEA respeta las expectativas de privacidad de las personas. Con esta finalidad:

- Si bien el flujo y la frecuencia de la transmisión electrónica de datos se supervisará de forma continuada, las comunicaciones electrónicas entre individuos identificables no se analizarán con la misma regularidad.
- La interceptación y/o la supervisión de comunicaciones electrónicas de una persona identificable, únicamente tendrán lugar como parte de una investigación definida a raíz de una petición por parte de la autoridad competente o de un asunto derivado de procedimientos disciplinarios de ORPEA, o cuando concurra una causa legítima y justifica que aconseje hacerlo.
- La petición de interceptar o supervisar las comunicaciones electrónicas de una persona identificable deberán ser presentadas por la Dirección General de ORPEA. En la mayoría de los casos, será el Manager de IT quien presente y autorice la petición.
- Cuando se hayan recogido datos (informes, ejemplos, estadísticas, etc.) en relación con las comunicaciones electrónicas de una persona identificable, éstos se gestionarán con el máximo cuidado y se pondrán en conocimiento del mínimo número de personas necesario para concluir la investigación.

5. Ejemplos

A continuación, se ofrece una orientación para interpretar la presente política. Los ejemplos no son exhaustivos. Cualquier aclaración u orientación que se pueda requerir, debería ser resuelta con antelación por el Manager de IT o un miembro del equipo de sistemas.

5.1. Correoelectrónico

5.1.1. Aceptable

- Comunicación relacionada con la actividad de ORPEA.
- Acceso de la Dirección para leer los buzones electrónicos de los empleados cuando exista la necesidad empresarial legítima de hacerlo (p. ej., si alguien está ausente y se esperan mensajes importantes).

5.1.2. Inaceptable

- Uso del correo electrónico para comunicaciones personales, no profesionales, salvo autorización previa escrita del Departamento de IT o Dirección.

5.1.3. Prohibido

- Enviar correos electrónicos, ya sea interna o externamente, o grabar o almacenar datos adjuntos o documentos que se pudieran considerar:
    - Difamatorios o potencialmentedifamatorios.
    - Acoso, victimización o intimidación, de acuerdo con la política de ORPEA.

- Violación de la política de igualdad de oportunidades de ORPEA.
- Discriminatorios
- Insultantes
- Pornográficos
- Obscenos
- Ilegales.
- Ofensivos
- Mal uso del logotipo o el nombre deORPEA
- El envío o comentario inadecuados de información de ORPEA, o de su actividad, fuera de la empresa.
- Instalar cuenta de correo profesional en dispositivo personal.

Nota: Cualquier persona que reciba material de cualquiera de las naturalezas mencionadas antes, deberá informar inmediatamente de ello a su encargado, al Manager de IT o al Departamento de Recursos Humanos. La omisión de esta obligación puede ser causa de acción disciplinaria.

5.2. Internet

5.2.1. Aceptable

- Acceso a sitios web del sector o relacionados con la actividad profesional.

5.2.2. Inaceptable

- Acceso a Internet para comunicaciones personales, no profesionales, durante la jornada laboral.
- Vinculación de gran parte de los recursos de Internet a actividades no profesionales, en detrimento del uso profesional genuino de Internet, incluyendo:
  - Dejar activos durante todo el día sitios web de actualización automática, p. ej. de noticias, de resultados deportivos, de negociación de acciones.
  - Acceso, descarga, distribución o almacenaje de imágenes, flujos de vídeo o de audio, con fines no profesionales.
  - Intentos reiterados de acceder a sitios web que se han bloqueado automáticamente por su contenido inadecuado.
  - Descarga de materiales sujetos a copyright sin la autorización del propietario o distribución de información, imágenes o texto ajenos a ORPEAque pudiera equivaler a una violación del copyright y que pudieran causar que ORPEA fuese objeto de acciones legales.
  - Inscripción a listas de correo, solicitud de información, suscripción a sitios personales o participación en chats o charlas interactivas por Internet, salvo que exista la necesidad profesional de hacerlo.
  - Formulación de comentarios imprecisos, infundados, discriminatorios, difamatorios u hostiles sobre cualquiera de los empleados, productos o servicios de ORPEA, ya sea interna o externamente.

5.2.3. Prohibido

- Mal uso del logotipo o el nombre deORPEA
- Envío de correos opinando o comentando asuntos o información relativos a ORPEA, en sitios web ajenos a ORPEA o mediante correo web.
- Descarga de software.
- Acceso deliberado a sitios que contienen material pornográfico, ofensivo u obsceno.

- Descarga de material pornográfico, ofensivo u obsceno.
- Grabación, almacenaje o reenvío de archivos o datos adjuntos no profesionales que pudieran ser considerados:
- Difamatorios o potencialmentedifamatorios.
- Acoso, victimización o intimidación de acuerdo con la política de ORPEA.
- Violación de la política de igualdad de oportunidades de ORPEA
- Discriminatorios
- Insultantes u ofensivos
- Pornográficos u obscenos
- Ilegales
- Descarga de utilidades P2P o de chat interactivo.
- Uso de sitios de correo web.

6. Notificación de violación de la presente política

Quien descubra una violación de la presente política, deberá informar de la misma alapersona encargada y/o al Manager Local de IT. La omisión de esta obligación puede ser considerada en sí misma como una violación de la política.

7. Violación del uso de la presente política

El incumplimiento o violación de la presente política constituye falta laboral, de acuerdo con lo que se establece en el procedimiento disciplinario de la empresa y normativa aplicable.

Igualmente la Empresa se reserva el ejercicio de las acciones legales ante cualquier jurisdicción derivadas del incumplimiento de esta Política y a fin de exigir las responsabilidades legales contra la persona incumplidora.