1. Objeto

El objeto de este documento es desarrollar la política de seguridad de la información y definir las reglas básicas para el uso aceptable de la información y del resto de activos asociados al tratamiento de esta.

2. Alcance

Este documento aplica a los siguientes activos:

- La información protegida, es decir, aquella información que permite identificar a personas físicas y/o jurídicas, y aquella relativa a la configuración de los sistemas de información y las redes de comunicaciones.
- Los asociados para el tratamiento de la citada información (software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar e instalaciones).

El tratamiento de la información se deberá realizar atendiendo todas las medidas de seguridad que garanticen su:

- Confidencialidad: es la propiedad de prevenir la divulgación de información a personas o procesos no autorizados. La confidencialidad es el acceso a la información únicamente por personas o procesos que cuenten con la debida autorización.
- Integridad: es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.
- Disponibilidad: es la propiedad de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas o procesos autorizados en el momento que lo requieran.

3. Normativa específica

3.1. Uso apropiado de los activos

La información y el resto de los activos asociados a la misma deberán ser utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de las personas usuarias.

Se prohíbe expresamente:

- El uso de los activos proporcionados por Grupo Azpiaran para actividades no relacionadas con su propósito.
- La conexión a la red de Grupo Azpiaran de equipos informáticos personales que no estén homologados.
- Introducir en los sistemas de información o la red corporativa de Grupo Azpiaran contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente en la red corporativa de Grupo Azpiaran cualquier tipo de malware (virus, gusanos, troyanos, programas espía, ransomware, …), dispositivo lógico,

dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos.

- Obtener otros derechos o accesos distintos a aquellos que Grupo Azpiaran le haya asignado.
- Acceder a las áreas restringidas de Grupo Azpiaran sin estar autorizado para ello.
- Descifrar las contraseñas, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Grupo Azpiaran
- Distorsionar o falsear los registros (logs) de los sistemas de información de Grupo Azpiaran
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otras personas usuarias, dañar o alterar los recursos informáticos de Grupo Azpiaran
- Destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos con información protegida.
- Guardar información protegida en las unidades locales de disco de los puestos PC de persona usuaria, excepto temporalmente la programación del proyecto de desarrollo en el que trabaja la persona.

3.2. Confidencialidad

La persona usuaria que tenga acceso a información de Grupo Azpiaran deberá considerar que dicha información, por defecto, tiene el carácter de protegida. Sólo se podrá considerar como información no protegida aquella información a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por Grupo Azpiaran

Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en que se encuentre.

Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior información protegida.

Se minimizará el número de informes en formato papel que contengan información protegida y se mantendrán los mismos en lugar seguro y fuera del alcance de terceras personas no autorizadas (p.e. bajo llave).

En el caso de que, por motivos directamente relacionados con el puesto de trabajo, la persona usuaria entre en posesión de información protegida contenida en cualquier tipo de soporte, deberá entender que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información. Asimismo, la persona usuaria deberá devolver el o los soportes mencionados, 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 su relación con Grupo Azpiaran

Todas estas obligaciones continuarán vigentes tras la finalización de su relación con Grupo Azpiaran

El incumplimiento de estas obligaciones podrá constituir un delito de revelación de secretos.

Además de las consideraciones ya mencionadas, para garantizar la seguridad de los datos de carácter personal, la persona usuaria deberá observar las siguientes normas de actuación:

- Solo podrá crear ficheros cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán guardados en unidades locales de disco de los puestos PC de persona usuaria y deberán ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon. Solo se podrá guardar temporalmente la programación del proyecto de desarrollo en el que trabaja la persona.
- No se albergarán datos de carácter personal en las unidades locales de disco de los puestos PC de persona usuaria.
- La salida de soportes y documentos fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable de seguridad (Responsable de Sistemas) cumpliendo las medidas de seguridad contenidas en este documento.
- Los soportes y documentos deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido a las personas autorizadas.
- La transmisión de información protegida a través de redes de telecomunicaciones (p.e. Correo electrónico) no se realizará en claro. Se deberá compartir la información protegida con terceros a través de SharePoint, cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceras personas.

3.3. Procedimiento disciplinario

La persona usuaria que incumpla la presente normativa se expondrá al inicio de un procedimiento disciplinario y, en su caso, sancionador.

Grupo Azpiaran puede implantar controles para verificar el cumplimiento de esta normativa, sin menoscabo del cumplimiento de la legislación vigente en materia de protección de datos de carácter personal y el derecho a la intimidad.

3.4. Devolución de los activos

La persona usuaria deberá devolver toda la información y los activos asociados para el tratamiento de esta que estén en su poder al finalizar su relación con Grupo Azpiaran.

Los accesos a la información y a los activos de tratamiento de esta de todas las personas usuarias deberán ser cancelados a la finalización de la relación con Grupo Azpiaran o deberán ser adaptados a los cambios de funciones producidos.

3.5. Seguridad física

El acceso a la documentación se limitará exclusivamente a las personas autorizadas.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación y de acuerdo con los requisitos de las organizaciones cliente. Estos criterios

deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que impidan su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, se adoptarán medidas que impidan el acceso de personas no autorizadas.

Mientras los soportes o documentos no se encuentren archivados en los dispositivos de almacenamiento establecidos en el apartado anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de esta deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Los armarios, archivadores u otros elementos en los que se almacenen los soportes o documentos deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los soportes o documentos.

La generación de copias o la reproducción de los documentos con datos de carácter personal especialmente protegidos (p.e. Salud) únicamente podrá ser realizada bajo el control de las personas autorizadas por el responsable de sistemas.

Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

3.6. Documentos, soportes y dispositivos portátiles

Los soportes, dispositivos portátiles y documentos que contienen información protegida deberán permitir identificar su contenido, ser inventariados y solo ser accesibles a las personas autorizadas por el responsable de seguridad.

La salida de soportes y documentos, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control de Grupo Azpiaran deberá realizarse a través del SharePoint corporativa autorizando a correos electrónicos individuales, no compartidos. Una vez finalizada la necesidad de compartir se revocará el acceso.

En el traslado de la documentación se deberán adoptar las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier documento o soporte que contenga información protegida deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

La identificación de los soportes que contengan información protegida se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a las personas

usuarias con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de las personas.

Asimismo, los soportes y dispositivos portátiles deberán estar cifrados, en especial cuando éstos se encuentren fuera de las instalaciones de la Organización.

3.7. Protección frente al malware

Se mantendrán los sistemas de información al día con las últimas actualizaciones de seguridad disponibles.

En la microinformática Apple, Windows y Android se dispondrá de software antimalware.

El software antimalware deberá estar siempre habilitado y actualizado.

3.8. Intercambio de información

Ninguna persona usuaria deberá ocultar o manipular su identidad en ninguna circunstancia.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicio para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.

En relación con el intercambio de información, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por los derechos de autor infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de información protegida a terceras personas no autorizadas.
- Transmisión o recepción de aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.

Todas las actividades que puedan dañar la imagen y reputación de Grupo Azpiaran están prohibidas en Internet y en cualquier otro lugar.

3.9. Uso del correo electrónico

Este recurso se utilizará con una finalidad profesional. Cualquier otro uso está prohibido.

Se prohíbe expresamente la interceptación y/o uso no autorizado de mensajes o direcciones de correo electrónico de otras personas usuarias.

La persona usuaria deberá rechazar cualquier mensaje de correo electrónico que provenga de fuentes no fiables, ya que podría contener virus o códigos maliciosos, spam, ...

La persona usuaria deberá evitar la divulgación innecesaria de la dirección de correo, principalmente no participando en cadenas de mensajes, por altruista que pueda parecer su objetivo.

3.10. Conectividad a Internet

Este recurso se utilizará con una finalidad profesional. Cualquier otro uso está prohibido.

En ningún caso deberá accederse a direcciones de Internet, de juegos, de contenido sexual, o que resulten ofensivas o atentatorias contra la dignidad humana o los derechos fundamentales.

3.11. Seguridad lógica

Las personas usuarias tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

Se establecerán mecanismos para evitar que una persona usuaria pueda acceder a recursos con derechos distintos de los autorizados.

El responsable de sistemas se encargará de que exista una relación actualizada de personas usuarias y perfiles, y los accesos autorizados para cada una de ellas.

Exclusivamente las personas autorizadas (administradoras) por el responsable de sistemas podrán conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por Grupo Azpiaran y la organización cliente.

En caso de que existan personas usuarias externas a la Organización deberán estar sometidos a las mismas condiciones y obligaciones de seguridad que las personas internas.

Se deberá establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de toda aquella persona usuaria que intente acceder a los sistemas de información y la verificación de que está autorizada.

El procedimiento de asignación, distribución y almacenamiento de contraseñas garantizará su confidencialidad e integridad.

Después de la intervención de una persona administradora de persona usuarias, los sistemas de información forzarán automáticamente al cambio de contraseña.

Los sistemas de información forzarán automáticamente al cambio de contraseña como mínimo una vez cada 90 días, siempre y cuando el sistema lo permita y si no existe posibilidad de activar MFA.

Las contraseñas vigentes se almacenarán de forma ininteligible.

La longitud mínima de las contraseñas deberá ser de 8 caracteres, alternando numéricos, alfanuméricos (mayúsculas y minúsculas) y especiales.

Los accesos autorizados temporales se configurarán para un corto período de tiempo y una vez expirado el mismo, se desactivarán automáticamente.

Los sistemas de información limitarán la posibilidad de intentar reiteradamente el acceso no autorizado a un máximo de 5 intentos.

3.12. Responsabilidades de la persona usuaria

3.12.1. Uso de contraseñas

La persona usuaria no deberá revelar bajo ningún concepto su identificador y/o contraseña a otra persona usuaria ni mantenerla por escrito a la vista, ni al alcance de terceras personas.

En caso de que el sistema de información no lo solicite automáticamente, la persona usuaria deberá cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema o intervenga alguna persona administradora.

En el caso que el sistema no lo solicite automáticamente, la persona usuaria deberá cambiar su contraseña como mínimo una vez cada 90 días, siempre y cuando el sistema lo permita y si no existe posibilidad de activar MFA.

La longitud mínima de la contraseña deberá ser de 8 caracteres.

Las contraseñas estarán constituidas por combinaciones de caracteres numéricos, alfanuméricos (mayúsculas y minúsculas) y especiales. Es recomendable utilizar las siguientes reglas para la selección de contraseñas:

- No utilizar palabras que hagan referencia a conceptos, objetos o ideas reconocibles (p.e. Fechas significativas, días de la semana, meses del año, nombres de persona usuaria, persona, teléfonos, ...).
- La contraseña deberá ser algo prácticamente imposible de adivinar, pero al mismo tiempo deberá ser fácilmente recordada por la persona usuaria (p.e. Usar el acrónimo de alguna frase o expresión, …).

Si la persona usuaria sospecha que su identificador y contraseña está siendo utilizado por otra persona, inmediatamente deberá proceder al cambio de su contraseña y notificar el incidente ITteam@azpiaran.com.

3.12.2. Equipo

La persona usuaria se deberá asegurarse de que su puesto PC de cumple las siguientes normas:

- Ante la inactividad, se bloquea automáticamente en un plazo máximo de 10 minutos.
- No dispone de:
  - Herramientas que puedan transgredir las medidas de seguridad.
  - Copias ilegales de programas.
  - Programas no homologados.
- Dispone de antimalware actualizado y activado en la microinformática en Apple, Windows y Android.
- Se mantiene al día con las últimas actualizaciones de seguridad disponibles.

3.12.3. Puesto de trabajo

La persona usuaria deberá respetar al menos las siguientes normas de escritorio limpio, con el fin de proteger los documentos en papel, soportes informáticos y dispositivos portátiles de almacenamiento y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:

- Almacenar bajo llave los documentos en papel y los medios informáticos, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Bloquear la sesión o apagar el puesto PC de persona usuaria al dejarlo desatendido.
- Proteger tanto los puntos de recepción y envío de información (correo postal, máquinas de scanner y fax) como los equipos de duplicado (fotocopiadora, fax y scanner).
- Retirar, sin retraso injustificado, cualquier información protegida una vez impresa.

- Destruir la información protegida una vez deje de ser necesaria.

3.13. Teletrabajo

El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regulará mediante la activación de las siguientes normas:

- No se permitirá la utilización de infraestructura (software, hardware y redes de comunicaciones) no controlada por Grupo Azpiaran
- Se establecerán criterios de autorización del teletrabajo en base a las necesidades del puesto de trabajo.
- Se establecerán las medidas necesarias para la conexión segura a la red corporativa.
- Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.
- Se controlará la revocación de derechos de acceso y devolución de la infraestructura tras la finalización del periodo de necesidad de esta.

3.14. Software

Exclusivamente las personas autorizadas (administradoras) por el responsable de administración podrá instalar software.

La persona usuaria deberá utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

Está terminantemente prohibido:

- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- El uso de software no autorizado por el responsable de administración.
- Desinstalar cualquiera de los programas instalados por Grupo Azpiaran

3.15. Incidentes

Por incidente se entiende cualquier evento o serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer la operativa de Grupo Azpiaran y atentan contra la presente normativa.

Cuando la persona usuaria detecte una posible vulnerabilidad, evento o incidente, deberá notificarlo inmediatamente a ITteam@azpiaran.com.

3.16. Cumplimiento normativo

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual.

La persona usuaria únicamente podrá utilizar material autorizado por Grupo Azpiaran para el desarrollo de sus funciones.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia de uso.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización por escrito de su persona titular o gestora de derechos.

Grupo Azpiaran únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su persona titular o gestora de derechos, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

Se garantizará el cumplimiento de la normativa vigente en materia de protección de datos de carácter personal en el tratamiento de los datos de personas físicas identificadas e identificables.