POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL PERSONAL

1.- INTRODUCCIÓN

Seguridad de la información, es el conjunto de medidas preventivas y reactivas que EL GRUPO BARNA PORTERS, emplea a para resguardar y proteger la información persiguiendo mantener la confidencialidad, disponibilidad e integridad de datos.

2.- ALCANCE

Esta política afecta a todos los miembros que integran la organización.

3.- OBJETIVOS

- Protección de la información contra cualquier acceso no autorizado.

- **Confidencialidad** de la información, especialmente aquella relacionada con los datos de carácter personal de los empleados y clientes.

Entendiendo confidencialidad como aquella que requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas.

El objetivo de la **confidencialidad** es, prevenir la divulgación **no autorizada de la información** sobre nuestra organización.

- **Integridad de la información.**

La **integridad**, supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá **modificar la información mediante autorización**.

El objetivo de la integridad es **prevenir modificaciones no autorizadas** de la información.

- **Disponibilidad de la información**

La **disponibilidad** supone que el sistema informático se mantenga trabajando sin sufrir ninguna **degradación en cuanto a accesos**. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información **deberá permanecer accesible a elementos autorizados**.

El objetivo es necesario **prevenir interrupciones no autorizadas** de los recursos informáticos.

3.- RESPONSABILIDADES

Equipo directivo:

Responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.

Responsable de Seguridad Informática:

Asesora al equipo directivo, y proporciona apoyo al personal de la organización

4.- POLÍTICAS RELACIONADAS

1/ Política de limpieza del puesto de trabajo.

2/ Política de software no autorizado.

3/ Política de copias de seguridad.

4/ Política de uso de servicios de mensajería.

5/ Política de uso de correo electrónico.

6/ Política de uso de dispositivos móviles corporativos.

7/ Política de Monitorización.

8/ Consecuencias del mal uso de los recursos.

Estas políticas sirven de apoyo para la identificación de riesgos, y deficiencias. Así como su debido tratamiento.

1/ Política de limpieza del puesto de trabajo.

La política de Escritorio y Pantalla Limpia de Información, define las medidas preventivas de protección y las buenas prácticas, con respecto de las estaciones de trabajo y escritorios de todo el personal que desarrolla sus actividades en las instalaciones del GRUPO BARNA PORTERS.

La finalidad de esta política es proteger los documentos de la Entidad, tanto los físicos como los digitales, y todo tipo de almacenamiento, al reducir los riesgos de acceso no autorizado a la información, y la pérdida y/o daño de la misma.

Este documento se basa en las buenas prácticas que permiten mantener el orden y la limpieza en el puesto de trabajo.

Cuidado de los puestos de trabajo :

Orden y Limpieza:

Los puestos de trabajo deben permanecer limpios y ordenados, y deben contar con lo necesario para poder desarrollar las funciones propias de su cargo, en particular se deben mantener únicamente aquellos implementos utilizados con mayor frecuencia. No se debe comer o ingerir bebidas en el puesto de trabajo.

Buen uso de los recursos:

Los recursos que forman parte del escritorio del personal, deben estar organizados y en condiciones de acceso a ellos de manera fácil, además de permanecer en buen estado.

Cerrar con llave escritorios a su caro. Para los casos en que aplique cerrar la puerta de la oficina, cerciorarse que así sea.

El ordenador deberá de ser apagado cuando deje de utilizarse.

No deben de dejarse documentos sobre el escritorio, de forma que quede información expuesta, evite agrupación de papeles de trabajo.

Bloqueo automático de protector de pantalla:

El bloqueo estándar debe activarse máximo con una espera de 5 minutos de inactividad en los equipos. Además deberán de cerrarse aplicaciones y bloquear la pantalla cuando se alejen del escritorio.

Protección de la información

Los equipos que queden ubicados cerca de zonas de atención y/o tránsito de público, deben situarse de forma que la información desplegada en sus monitores no pueda ser visualizada por personas externas, aplicando el bloqueo automático de protector de pantalla. Los documentos en papel que contengan información confidencial o sensible, se deberán guardar en lugar seguro, bajo llave, en gabinetes u otro tipo de mobiliario seguro.

Manejo de dispositivos móviles y computadores portátiles Todos los dispositivos móviles deben ser llevados por sus dueños, con las máximas medidas de seguridad posibles como contraseñas de autenticación. Todos los ordenadores portátiles deben estar siempre con código de seguridad para su protección, éstas deben tener una clave de seguridad que solo el responsable del equipo debe conocer.

Elementos de acceso y almacenamiento removibles: El personal que tengan asignadas llaves físicas de armarios, son responsables del uso y custodia de la información allí almacenada y de los recursos físicos que se encuentren en éstas; de ser posible estas llaves deben ser guardadas en cajas fuertes o en áreas de acceso restringido. Nunca dejar en el escritorio llaves, éstas deben permanecer siempre controladas por el personal responsable. En caso de tener permisos para utilizar medios removibles como CDs, DVDs y USB no dejarlos conectados en ausencia.

Nunca escribir las contraseñas en notas autoadhesivas, ni tratar de esconderlas en los puestos de trabajo.

Revisar que no queden documentos en cola de impresión y verificar que en las impresoras no queden trabajos impresos, fax, escáner y demás máquinas donde pueda haber papel con información confidencial, privada o restringida. Triturar impresiones con datos sensibles una vez utilizados y que no se necesiten.

Cumplimiento de la política de escritorio limpio Todo empleado es responsable por el cumplimiento de las normas y estándares contenidos en este documento, además, tiene la obligación de informar, si observan incumplimiento de esta política por parte de otras personas, en caso de que se esté exponiendo la confidencialidad, integridad y disponibilidad de la información. La omisión de esta norma se considera incumplimiento de las obligaciones laborales por parte del trabajador.

AL FINALIZAR LA JORNADA LOS ORDENADORE DEBEN QUEDAR APAGADOS, EN EL CASO DE QUE SEA NECESARIO QUE PERMANEZCAN ENCENDIDOS, LA PANTALLA DEBE ESTAR BLOQUEADA.

2/ Política de software no autorizado.

La instalación y uso de software ilegal en algún dispositivo incrementa los riesgos de infección por malware.

Así mismo, para evitar fugas de información y garantizar la privacidad de los datos de carácter personal , la empresa deber determinar y controlar qué software está autorizado para el tratamiento de la información.

La organización mantiene un registro actualizado de las licencias disponibles del software autorizado., que incluye:

- Nombre y versión del producto, fecha de adquisición, vigencia de la licencia, tipo de licencia, número de usuarios permitidos por licencia, número de licencias adquiridas por cada software.

La organización cuenta con un responsable informático que se encargará de la instalación, actualización y eliminación del software de los equipos de la empresa.

Ningún usuario de la organización podrá realizar copias del software puesto a su disposición, sin el debido consentimiento.

La organización se reserva el derecho de auditar o inspeccionar en cualquier momento los equipos de los usuarios para verificar que se cumple esta política.

3/ Política copias de seguridad

Una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos.

Sin embargo, en el ámbito empresarial podríamos definir la copia de seguridad como la salvaguarda de nuestro negocio, una medida indispensable para garantizar su continuidad y conservar la confianza que nuestros clientes han depositado en nuestra organización. De lo contrario, podríamos proyectar una imagen negativa y generar desconfianza.

Clasificación de la información:

- Por el nivel de accesibilidad o confidencialidad
- Por su utilidad o funcionalidad
- Por el impacto, en caso de robo, borrado o pérdida

Por el nivel de accesibilidad o confidencialidad:

- Accesible solo por la dirección o personal concreto.
- Interna: accesible solo al personal de la empresa.
- Pública: accesible públicamente.

Por su utilidad o funcionalidad:

- Información de clientes y proveedores
- Información de compras y ventas
- Información de personal

Por el impacto en caso de robo, borrado o pérdida:

- Daño de imagen
- Consecuencias legales
- Consecuencias económicas
- Paralización de actividad

CATEGORÍA	DEFINICIÓN	TRATAMIENTO
Confidencial	Información especialmente sensible para la organización.	Su acceso será restringido únicamente a la dirección y a aquellos empleados que necesiten conocerla para desempeñar sus funciones. Las personas que tengan acceso se mantendrán registradas, y causarán baja

		de registro en cuanto causen baja en la organización, o vean modificado su puesto de trabajo, que implique la innecesariedad de acceder a dicha información. El acceso se realizará mediante un usuario y contraseña, que no podrá facilitarse a personas ajenas, ni terceros. En caso de sacar la información de las instalaciones de la empresa, deberá de ser registrado, donde constará fecha, y persona de entrega, así como destino. Unicamente podrá sacar la información las personas autorizadas por el responsable del departamento correspondiente, y si es posible siempre se empleará la mensajería interna supervisada.
Interna	Información propia de la empresa, accesible para todos sus empleados.	Esta información solo podrá ser accesible a la plantilla, y nunca podrá difundirse a terceros salvo autorización expresa de la dirección de la empresa. La mayoría de esta información se podrá localizar en la aplicación SERVIAP, o bien en el COMÚN público de la organización.
Pública		

	Cualquier material de la empresa sin restricciones de difusión. Por ejemplo web o material comercial	Esta información no está sujeta a ningún tipo de tratamiento especial.

Periodicidad y tipo de copias

- Completa

Consiste en hacer una copia de todos los datos de nuestro sistema en otro soporte.

Copia completa al NAS, cada domingo a las 22.45h

HYperV (sistema completo, datos incluidos)

Cada domingo a las 21.45h al NAS.

- Incremental

Solo copia los datos que han variado desde la última copia de respaldo realizada.

Cada 4 horas entre las 6.30h y las 23.00h

- Diferencial

Es similar a una copia incremental en la primera vez que se realiza, ya que se copiarán todos los datos que hayan cambiado desde el respaldo anterior. Si bien, cada vez que se vuelva a lanzar, no solo se copiarán los datos que se hayan modificado desde la última copia, si no todos los que se hayan modificado desde la última copia completa realizada.

Cada 8 horas entre las 8.00h y las 23.15h

Las personas usuarias no deben realizar copias de la información clasificada como confidencial o secreta, al margen de los procedimientos de backup definidos, sin autorización de la persona propietaria de la misma.

Las copias temporales se deben destruir una vez finalizada la necesidad de su uso.

Las personas usuarias no deben almacenar información en sus equipos personales de trabajo. Debe ser almacenada en los servidores de datos del grupo.

Donde se almacenan las copias de seguridad

Se almacena en servidor propio, situado en las instalaciones centrales sitas en calle Arizala 43-45, bajos. En el interior de la central receptora de alarmas, blindada contra intrusiones ajenas.

4/ Política de uso de servicios de mensajería instantánea.

El servicio de mensajería instantánea, se conoce también como “chat”, que es un canal de comunicación en tiempo real.

Su uso de ser prudente y mesurado, y únicamente para apoyar las comunicaciones propias del servicio.

Está totalmente prohibido emplear este canal para compartir información confidencial, restringida, secreta o de cualquier otra índole, entre los usuarios, clientes , empleados o proveedores.

Este servicio únicamente se podrá utilizar para fines laborales.

No se permite el abuso de la mensajería instantánea en el trabajo empleándola para extensas conversaciones personales.

Está prohibido el uso de este sistema para expresas opiniones difamatorias, ofensivas, obscenas, racistas, calumniadoras y sexuales sobre superiores, compañeros o subalternos. De igual aplicación, para clientes, proveedores, y demás entidades con quien haya comunicación.

No se podrán transferir archivos por medio de este sistema.

No es aconsejable compartir información o datos personales, a través de este medio, ni tampoco contraseñas o números de tarjeta de crédito, cuentas bancarias o números de teléfono.

Uso indebido del servicio:

- Emplear la comunicación con fines personales.
- Realizar cualquier tipo de acoso, difamación, calumnia, intimidación u otra forma de actividad hostil
- Compartir información del grupo, sin autorización.
- Compartir documentos o archivos sin tomas medidas de precaución adecuadas.

El grupo de soporte tecnológico, puede monitorear el intercambio de mensajes instantáneos con el fin de asegurar el buen uso. Además de tener el derecho a acceder y revisar los contenidos de los mensajes de los usuarios

5/ Política de uso de correo electrónico.

- **Instrucciones generales de uso del correo electrónico**

El personal al servicio de BARNA PORTERS S.L. tiene que hacer un buen uso del correo electrónico que le ha sido atribuido para el ejercicio de sus funciones. Con este objetivo, tiene que cumplir estas normas. Cada persona trabajadora que tiene una cuenta de correo asignado se configura como persona usuaria de estos sistemas y es responsable de estos recursos que tiene asignados y de todas las acciones que se lleven a cabo en su utilización.

- **Usos admitidos del correo electrónico**

El uso de la cuenta de correo electrónico facilitado por BARNA PORTERS S.L. se tiene que limitar al desarrollo de las funciones propias del puesto de trabajo. De acuerdo con esto: 1. Sólo se puede utilizar con finalidades privadas si se trata de un uso por motivos personales o domésticos, que no sea abusivo y no perjudique la seguridad de los sistemas de información de

la organización, ni el normal desarrollo de las funciones encomendadas. 2. No se puede utilizar para actividades profesionales ajenas a las tareas encomendadas.
3. Las personas usuarias que tengan atribuida la gestión de cuentas de correo genéricas asociadas a determinados trámites o a unidades administrativas (p. ej. consultes@.....cat) en ningún caso pueden hacer un uso por motivos personales, ni pueden facilitar esta dirección con finalidades personales.
4. No se permite el uso del correo electrónico facilitado para contratar servicios personales no relacionados con la actividad profesional. Se prohíbe la configuración de cuentas de correo en los ordenadores de BARNA PORTERS S.L., fuera de las cuentas facilitadas por la misma entidad. No se permite el uso de programas chat, redes sociales, mensajería instantánea, etc. durante la jornada laboral, a menos que estén vinculados al ejercicio de las funciones encomendadas.

- **Gestión del buzón de correo**

Corresponde a cada usuario velar para que la gestión de la información contenida en su correo electrónico sea adecuada. Por ello:
1. Hay que revisar y vaciar periódicamente la bandeja de entrada y, si procede, la de salida, como mínimo, una vez cada 15 días. Hay que eliminar los mensajes que no se tengan que conservar y archivar el resto de mensajes en la carpeta o subcarpeta adecuada, especialmente los que pueden tener un contenido personal.
Los mensajes que formen parte de un procedimiento administrativo, u otros que se tengan que conservar, sólo se pueden eliminar de la cuenta de correo si previamente han sido debidamente archivados en el expediente correspondiente.
2. Los correos electrónicos con finalidades privadas que se conserven se tienen que señalar como tales, ya sea mediante una denominación o marca que los permita identificar, ya sea mediante la creación de una carpeta específica para correos privados donde se guarden este tipo de mensajes.
3. Hay que borrar también, periódicamente, los mensajes de la papelera o carpeta de eliminados.
5. Las direcciones de los correos electrónicos del personal al servicio de BARNA PORTERS S.L. se publican en la intranet corporativa. Estas direcciones se pueden utilizar:
a) Para las comunicaciones entre el personal vinculadas al ejercicio de las funciones respectivas.
b) Por los representantes de los trabajadores para enviar información relacionada con la actividad sindical en la empresa. Las personas trabajadoras pueden oponerse a la utilización de la dirección con esta finalidad, dirigiéndose directamente al sindicato de que se trate o bien a BARNA PORTERS S.L.
En cambio, estas direcciones no se pueden facilitar a terceras personas ajenas a la organización, a menos que resulte necesario para el ejercicio de alguna de las funciones encomendadas. Conviene utilizar el derecho de cancelación delante de terceras personas ajenas a la empresa que utilicen indebidamente el dato relativo a la dirección de correo electrónico profesional.

- **Medidas de seguridad**

Medidas generales
Las personas usuarias tienen que cumplir las medidas de seguridad siguientes:
a) Guardar el usuario y la contraseña de acceso a la cuenta de correo de forma segura y no facilitarlos a otras personas, ni siquiera a efectos de mantenimiento del sistema.
b) No utilizar una contraseña fácilmente deducible.

c) No hacer uso de la opción de guardar la contraseña que se ofrece al usuario para evitar reintroducirla en cada conexión.
d) Bloquear el acceso a la cuenta de correo, en caso de ausentarse del puesto de trabajo durante la jornada.
e) No seguir cadenas de mensajes piramidales.
f) No desactivar los filtros de correo y las opciones de seguridad activadas por el administrador del sistema.
g) No utilizar la opción de vista previa.
h) No abrir mensajes sospechosos.
i) No enviar, reenviar o responder mensajes de correo que contengan datos sensibles, sin la autorización de la Dirección.
j) En caso de detectar una incidencia durante el uso del correo electrónico, la persona trabajadora lo tiene que poner en conocimiento del responsable de seguridad de forma inmediata.

Firma electrónica
Hay que hacer uso de la firma electrónica cuando sea necesario para garantizar la autenticidad y la integridad del correo electrónico.
Se puede firmar electrónicamente un mensaje con el certificado electrónico facilitado por la empresa, si se cumplen las dos condiciones siguientes:
a) El correo se envía asociado a la identidad de una persona. No es aplicable, por lo tanto, en casos de correos genéricos.
b) La comunicación se efectúa en ejercicio de las funciones atribuidas. Quedan excluidos, por lo tanto, los correos personales o privados.

Mensajes cifrados
Los mensajes de correo electrónico se tienen que cifrar cuando contengan:
• Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
• Datos obtenidos con fines policiales sin el consentimiento de las personas afectadas.
• Datos derivados de actos de violencia de género.

- **Otras normas de buen uso del correo electrónico**

1. Utilizar la opción de copia oculta (CCO) cuando se envíe un mensaje a más de una persona destinataria que no forme parte de la empresa.
2. Utilizar la opción de reenviar sólo en los casos en que la persona destinataria pueda acceder tanto al emisor del mensaje como a su contenido, y a toda la información de la cadena de correos que forman parte de ella.
3. Eliminar el pie de firma, si se envía un mensaje privado desde el correo profesional.

- **Ausencia de la persona trabajadora**

En caso de ausencia programada superior a 5 días, se puede activar el mensaje de ausencia de oficina para facilitar otra dirección de contacto que garantice la continuidad de la actividad. El texto del mensaje de ausencia de oficina será el siguiente: *El texto del mensaje de ausencia de oficina, será el que la compañía acuerde y no podrá modificarse unilateralmente.*
Previamente a la ausencia, conviene:
1. Guardar la información personal o privada en una carpeta personal.
2. Transferir la información necesaria para continuar con la actividad durante la ausencia.

- Cese de la relación laboral

La empresa puede cancelar la prestación del servicio de correo en el momento en que finalice la relación contractual con el empleado o cuando el usuario esté haciendo un mal uso de él. La persona trabajadora tiene derecho a obtener los mensajes personales que en aquel momento estén almacenados en la carpeta de mensajes personales que designe o que se puedan identificar como tales. El resto de mensajes se pueden analizar para determinar si resultan necesarios para la continuidad de la actividad o bien si se pueden suprimir.

- **Acceso al correo electrónico fuera del puesto de trabajo**

Cuando se utilice el correo electrónico facilitado por la empresa fuera del puesto de trabajo hay que tener en cuenta:

a) No hacer uso de la opción de guardar la contraseña, cuando se utilicen ordenadores de uso compartido.

b) Borrar el historial de navegación y cerrar la sesión, al finalizar, siempre que se utilice un ordenador de uso compartido para acceder al correo vía web.

c) Utilizar programas antivirus.

d) Utilizar usuario y contraseña para bloquear los dispositivos móviles desde donde se pueda utilizar el correo electrónico profesional.

e) Utilizar mecanismos de cifrado del contenido del dispositivo móvil.

- Buenas prácticas en el uso del correo

En relación con los destinatarios

• Revisar las direcciones de los destinatarios, antes de enviar el mensaje.

• Valorar la utilización de la opción de copia oculta, para enviar un correo electrónico a múltiples destinatarios.

• Cuando se reenvía un correo electrónico, eliminar las direcciones de los anteriores destinatarios para no difundir, de forma injustificada, direcciones de correo de terceros.

En relación con el asunto

• Identificar clara y concisamente el asunto.

• No incluir datos personales en el asunto.

• Evitar palabras o expresiones que puedan activar los programas anti inundación (anti spam).

En relación con el contenido

• Revisar la posibilidad de revelar el contenido del mensaje antes de enviarlo.

• Utilizar el pie de firma automático de los mensajes de correo electrónico, de acuerdo con el modelo corporativo establecido, que incluye la cláusula de confidencialidad. Cuando se trate de mensajes con finalidades personales, hay que suprimir el pie de firma.

• Organizar los mensajes enviados y recibos en carpetas. Mantener la bandeja de entrada actualizada.

En relación con los archivos adjuntos

• Revisar la posibilidad de revelar el contenido de los archivos adjuntos antes de enviarlos.

• Evitar enviar archivos excesivamente grandes. El volumen máximo previsto será el que la empresa asigna a cada trabajador/a. Cuando sea superior, los archivos se pueden comprimir.

- **Acceso a la cuenta de correo electrónico por parte de la empresa**

La empresa puede hacer controles automatizados sobre el uso del correo electrónico, con el fin de velar por el normal funcionamiento del sistema (volumen de tráfico, volumen de los mensajes enviados, etc.).
Sólo se accederá al contenido de los mensajes o de los documentos adjuntos cuando no se puedan utilizar otros mecanismos menos intrusivos, en los siguientes casos:
a) Para llevar a cabo tareas de mantenimiento o vinculadas a la seguridad del sistema. En estos casos, se informará a la persona trabajadora de las tareas que se tienen que realizar y se le ofrecerá la posibilidad de estar presente.
b) Para comprobar, en el seno de una información reservada o de un procedimiento disciplinario, el uso del correo electrónico, en aquellos casos en que haya indicios de que la persona trabajadora ha hecho un mal uso de él. En este caso, hace falta la autorización del jefe de recursos humanos a petición del instructor del procedimiento. El acceso se tiene que hacer en presencia de la persona trabajadora o, si procede, de un representante del personal.
c) Para garantizar la continuidad laboral en caso de ausencia imprevista de la persona trabajadora. Si, por una necesidad improrrogable ligada a la actividad laboral, hay que acceder al contenido de los mensajes del correo electrónico de la persona trabajadora ausente, ésta puede delegar en otra persona trabajadora para verificar la forma como se lleva a cabo el acceso. No se puede acceder en ningún caso, por este motivo, a los mensajes que la persona trabajadora haya señalado como privados o que tenga almacenados en una carpeta identificada como privada.

6/ Política de uso de dispositivos móviles corporativos.

Se entienden como tales aquellos dispositivos tales como ordenadores portátiles, tablets, y teléfonos móviles, propiedad de la empresa.

Las tecnologías de la movilidad permiten que el empleado pueda desempeñar su trabajo, como si estuviera en las instalaciones de la empresa, acceso al correo, aplicaciones corporativas, información confidencial etc…

Pero estos dispositivos mantienen un alto riesgo de pérdida o robo.

Sistemas de control:

- Procedimiento de solicitud y asignación de dispositivos móviles corporativos a través de responsable de departamento, dirigido a dirección y posteriormente a departamento informático y tecnológico.
- Mantenimiento de un registro de los portátiles asignados.
- Sistema de tickets internos a través de SERVIAP, como formulario de incidencia o cambios.
- Configuración de los BIOS mediante contraseña.
- Comunicación al usuario de si el dispositivo dispone de software de localización.
- Prohibición de almacenar información no corporativa.
- Evitar la conexión a redes no conocidas. Solo conexión a redes privadas.
- Notificación inmediata al personal técnico responsable, cualquier sospecha de virus o software malicioso.
- No exponer el equipo a altas temperaturas. No descuidarlo en lugares públicos, No se deja visible en el coche o fácilmente accesible.

7/ Monitorización.

Las personas usuarias conectadas y a la infraestructura del grupo BARNA PORTERS, son conscientes de que los sistemas de información usados para el acceso a/desde/dentro de la red del grupo son propiedad exclusiva de este. Por lo que los usuarios entienden que no tienen el derecho de propiedad y confidencialidad en su uso. Lo que significa que GRUPO BARNA PORTERS puede en todo momento ejercer su derecho a procesar controles basados en la identidad de la persona usuaria y el contenido de sus comunicaciones, respetando la legalidad vigente, y sin la necesidad de informar a la persona afectada.

Todo ello con la finalidad de asegurar el correcto funcionamiento y uso de los recursos informáticos por parte de las personas usuarias.

En caso de que EL GRUPO BARNA PORTERS detecte mal uso por parte de alguna persona usuaria, se comunicará a ésta. Si se detectase un uso malintencionado o fraudulento, se podrán ejercer las acciones que se estimen oportunas.

EL GRUPO BARNA PORTERS, podrá realizar controles para observar el correcto cumplimiento de las normas vigentes.

8/ Consecuencias del mal uso de los recursos.

Las personas usuarias, cuando se les solicite, deben de colaborar con los responsables de seguridad.

En el caso de que la persona responsable detectara la existencia de un mal uso de los recursos y éste proceda de las actividades de un apersona usuaria determinada, pueden tomarse las siguientes medidas para proteger a otras personas, redes o equipos:

- Notificar la incidencia a la persona usuaria o Responsable.
- Suspender o restringir el acceso o uso del servicio mientras dure la investigación.
- Con el permiso del responsable de seguridad, inspeccionar ficheros o dispositivos de almacenamiento de la persona usuaria implicada.
- Informar a Dirección.

Medidas sancionadoras:

En caso de que fuera necesario, la Gerencia del GRUPO BARNA PORTERS adoptará las medidas que estime oportunas hacia las personas infractoras de esta política, según lo establecido en la legislación vigente.