POLÍTICA DE SEGURIDAD DEL PERSONAL PARA EL TRATAMIENTO DE DATOS PERSONALES

1.- ÁMBITO DE APLICACIÓN

El Responsable del tratamiento está comprometido en implantar una cultura de privacidad en la organización por lo que necesita que las personas autorizadas a tratar datos personales estén informadas del tratamiento de datos y se responsabilicen del mismo.

A toda persona autorizada para tratar datos personales se le exige que lea, comprenda, cumpla y haga cumplir esta Política de seguridad para proteger los datos que forman parte del tratamiento que le ha sido encomendado.

Esta Política de seguridad establece las obligaciones y procedimientos a seguir por el personal de la organización, tanto propio como externo, que trata datos personales en el desarrollo de su actividad y se basa en lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR) y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD).

En este sentido, para velar y hacer cumplir esta Política, la organización ha designado un Responsable de seguridad que estará a disposición de todo el personal y se encargará de coordinar, controlar, desarrollar y verificar el cumplimiento de las citadas normativas.

2.- CONCEPTOS BÁSICOS

Para proporcionar una mejor comprensión de la protección de datos, definimos los principales conceptos básicos:

Estructura del tratamiento:

- **Datos personales**: Información relativa a una persona física por la cual pueda determinarse su identidad.
- **Tratamiento**: Cualquier operación realizada sobre datos personales: obtención, acceso, intervención, transmisión, conservación y supresión.
- **Interesado**: Persona física sometida al tratamiento de sus datos personales.
- **Fichero**: Conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado.
- **Responsable del tratamiento**: Organización que determina los fines y los medios del tratamiento.
- **Personal autorizado**: Persona autorizada por el Responsable para realizar un tratamiento de datos mediante un compromiso de confidencialidad.

Categorías de datos:

- **Básicos**: Datos que no correspondan a categorías Penales o Especiales, por ejemplo: nombre, dirección, email, teléfono, edad, sexo, firma, imagen, aficiones, patrimonio, datos bancarios, información académica, profesional, social, comercial, financiera, etc.
- **Penales**: Datos relativos a la comisión de infracciones administrativas o penales, o los que puedan ofrecer una definición de características de personalidad, etc.
- **Especiales**: Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.

3.- PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Los principios fundamentales para realizar un tratamiento de datos son:

- **Licitud**: lealtad y transparencia con el interesado.
- **Limitación de los fines**: tratados para fines determinados.
- **Minimización de los datos**: solo se deben obtener los datos necesarios para alcanzar los fines.
- **Exactitud**: actualizados.
- **Limitación del plazo de conservación**: guardados durante no más tiempo del necesario para conseguir los fines.
- **Integridad y confidencialidad**: aplicación de medidas de seguridad para la protección de los datos en todas las fases del tratamiento.
- **Responsabilidad proactiva**: se debe poder demostrar el cumplimiento de todos los principios de protección de datos.

Consentimiento para realizar un tratamiento de datos

- Para tratar datos deberemos obtener el consentimiento explícito del interesado y guardar el documento probatorio que lo acredite.
- Cuando obtengamos los datos de terceros, deberemos asegurarnos que la comunicación es lícita y guardar el documento probatorio que lo acredite.
- No es necesario obtener el consentimiento del interesado cuando el tratamiento se base en una obligación legal (por ejemplo, para emitir una factura).

Información del tratamiento al interesado

Deberemos facilitar la siguiente información al interesado:

- La identidad y los datos de contacto del Responsable del tratamiento
- Los fines del tratamiento.
- La base jurídica del tratamiento.
- El plazo de conservación de los datos o los criterios que lo determinen.
- Los derechos que asisten al interesado.
- Y si existen:
    - Los destinatarios o categorías de destinatarios de los datos.

- La transmisión de datos a países u organizaciones establecidas fuera de la UE.

Responsabilidad del tratamiento

El tratamiento de datos se podrá realizar por organizaciones externas siempre y cuando exista una autorización expresa del Responsable y se haya suscrito un contrato para realizar dicho tratamiento conforme a la legislación vigente. Para conocer qué empresas o terceros están autorizados a la cesión de datos, deben dirigirse al Responsable de seguridad.

Las organizaciones externas pueden ser:

- **Encargados del tratamiento**: Organización que trata datos personales por cuenta del Responsable.
- **Destinatarios de datos**: Organización distinta del Encargado, que recibe una comunicación de datos personales del Responsable.

Medidas de seguridad

La organización ha implementado medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado a los riesgos que pueda tener el tratamiento como consecuencia de la destrucción accidental o ilícita de datos, la pérdida, alteración o comunicación no autorizada y el acceso a los datos cuando son transmitidos, conservados u objeto de algún otro tipo de tratamiento.

El personal deberá velar por la seguridad de los datos tratados por la organización y comunicará al Responsable cualquier operación de tratamiento que pueda suponer un riesgo que afecte la protección de datos o los intereses y libertades de los interesados.

Cualquier diseño de una nueva operación de tratamiento o actualización de una operación existente deberá garantizar antes de su implantación, la protección de datos personales y el ejercicio de los derechos de los interesados en todas las fases del tratamiento: obtención, acceso, intervención, transmisión, conservación y supresión.

4 - FUNCIONES Y OBLIGACIONES DEL PERSONAL

El personal deberá actuar en todo momento conforme las instrucciones detalladas en el acuerdo de confidencialidad suscrito con la organización y las establecidas en esta Política de seguridad. Para ello se establecen las siguientes medidas de protección de datos que el personal se obliga a cumplir expresamente:

Organización de la información

Se deberán clasificar los datos de manera que se puedan ejercer los derechos de los interesados: acceso, rectificación, supresión y portabilidad de los datos y limitación u oposición al tratamiento.

Conservación de los datos

Se deberán conservar los datos en el mobiliario y departamento destinados a tal fin. Para tratamientos automatizados se guardarán los archivos en los soportes, carpetas o directorio de red indicados por el Responsable de seguridad.

No está permitido conservar datos en el escritorio físico o digital. Solo se permite su tratamiento temporal en dicho escritorio para realizar las operaciones que lo precisen debiendo ser conservados en el lugar apropiado al término de la jornada laboral.

Acceso a la información

Se deberán aplicar los mecanismos de acceso restringido a la información que haya implementado la organización, salvaguardando las claves de acceso de toda divulgación o comunicación a otras personas.

Cada persona sólo está autorizada a acceder a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones.

Se restringirá el acceso a los equipos informáticos mediante procedimientos que puedan identificar y autenticar la persona que accede a los mismos. Los nombres de usuario y contraseña tendrán la consideración de datos personales intransferibles.

Procesamiento de datos

Los soportes documentales e informáticos deberán estar dispuestos de tal forma que no sean accesibles a personas no autorizadas.

Si una persona abandona su puesto de trabajo temporalmente, deberá ocultar los documentos y bloquear el ordenador, de modo que se impida la visualización de la información con la que estaba trabajando.

Cuando se utilicen impresoras o fotocopiadoras, después de la impresión de trabajos con información de carácter personal, se debe recoger de manera inmediata, o imprimir de forma bloqueada, asegurándose de no dejar documentos impresos en la bandeja de salida.

Transporte de soportes

El transporte de soportes que contengan datos personales deberá realizarse únicamente por personal autorizado o empresas externas contratadas para tal fin por el Responsable del tratamiento.

Eliminación de documentos

Cualquier documento físico o soporte digital que quiera ser eliminado y que incluya datos personales, debe ser destruido con la destructora o retirado por una empresa homologada de destrucción de documentos.

Copia de seguridad y recuperación de datos

El personal deberá almacenar toda la información tratada en el directorio de red correspondiente indicado por el Responsable de seguridad, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se sometan los procedimientos de copias de seguridad aplicados por la organización.

Protección de datos

Se deberán aplicar las medidas de protección de datos establecidos por la organización relativos a la seguridad del tratamiento como pueden ser la seudonimización o cifrado de datos o advertencias de intrusión como antivirus, antispam, etc.

Gestión de incidencias

Se considera una incidencia a cualquier violación de la seguridad que ocasione la destrucción accidental o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de datos personales.

El personal tiene la obligación de notificar sin demora injustificada, cualquier incidencia que tenga conocimiento al Responsable de seguridad para su conocimiento y aplicación de medidas correctivas para remediar y mitigar los efectos que hubiera podido ocasionar. Las incidencias deberán documentarse por la persona que la notifica con una descripción detallada de la misma y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella.

El conocimiento y no notificación de una incidencia por parte del personal se considerará una falta contra la seguridad de los datos y podrá suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que el Responsable se vea obligada a atender como consecuencia de dicho incumplimiento.

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

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 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 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.

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.

- El usuario tiene la obligación de informar inmediatamente al Departamento de Informática en caso de robo o pérdida del dispositivo móvil.

El usuario deberá siempre poner a disposición de la empresa su dispositivo, a requerimiento de esta. Así como entregarlo, en el supuesto de cesar en su prestación de servicios para la empresa.

Geolocalización

La empresa podrá introducir mecanismos de geolocalización a los empleados, insertados en los vehículos propiedad de la empresa, y puestos a disposición de los empleados en ejercicio de su trabajo, así como en software de control de cumplimiento horario.

Cualquiera de los mecanismos empleados, solo podrá ser empleado en horario laboral. Respetando la intimidad del trabajador, en horario extra laboral.

Cesión de datos

La empresa no va a ceder sus datos personales a terceros, salvo en caso de que sea necesario cumplir con una disposición legal o sea necesario para la prestación del servicio solicitado en cuyo caso, la empresa como Responsable del Tratamiento se compromete ceder solo aquellos datos que sean estrictamente necesarios y a vigilar que los destinatarios de los mismos implanten las medidas de seguridad necesarias para asegurar la privacidad, seguridad e integridad de los mismos.

El Responsable del Tratamiento no va a realizar Transferencias Internacionales de Datos.

Con la finalidad de dar cumplimiento a los contratos mantenidos con la clientela, la empresa, a requerimiento del cliente, podrá ceder información de datos identificativos de su personal, que únicamente podrán ser empleados para el estricto control y verificación del cumplimiento de las condiciones contractuales pactadas.

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.

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.

Consideraciones generales

El personal mantendrá una actitud proactiva con la empresa respecto a la seguridad de la información, entendiendo la importancia prioritaria del cumplimiento de todas las directrices establecidas.

Grup Barnaporters realizará sesiones de concienciación y formación para garantizar que todo el personal tiene los conocimientos suficientes respecto a la seguridad de la información.

Bajo ningún concepto se podrá copiar información de la empresa y trasladarla fuera de las instalaciones a personal ajeno a la empresa. Cualquier copia de información deberá solicitarse al Jefe/a inmediatamente superior para que de su autorización.

Durante el transporte de información fuera de los límites físicos de nuestra organización, no se permitirá que personas no autorizas tengan acceso a ésta, se realice un uso indebido o se deteriore de ninguna forma. En caso contrario se aplicará la política sancionadora especificada en el punto 10 de este documento.

Semestralmente y de forma automática el usuario deberá modificar la clave de acceso a su ordenador, sin poder repetir la última contraseña. No se permite, en ningún caso, comunicar esta clave de acceso. Dicha clave deberá incorporar mayúsculas y minúsculas, letras y números y un número mínimo de ocho caracteres.

En el caso de ser responsable de atender alguna visita de personal externo, se las deberá acompañar en todo momento.

Si eres personal que trabaja en las zonas restringidas de la empresa, es decir, zonas donde se requiera reconocimiento biométrico para la apertura de la puerta, deberás garantizar que:

- Las puertas queden cerradas a tu paso
- Conectar o desconectar la alarma si eres la última persona en entrar o abandonar las instalaciones (solo para el personal que dispone de códigos de alarma).
- No dejar acceder a otro personal a las zonas seguras si no es con un propósito adecuado.

Todos los equipos de la empresa disponen de una sistemática de bloqueo de equipo desatendido, es decir, la pantalla se bloquea pasados tres minutos sin actividad. Esto garantiza la seguridad de tu equipo y los datos que contiene, no puedes modificar esta sistemática de bloqueo.

Como personal de la empresa si debes intercambiar información con otros trabajadores solo debe ser aquella que sea necesaria para las funciones que desarrolla. En caso de duda debes solicitar autorización a tu Jefe/a de Departamento.

Si detectas cualquier incidencia, punto débil en nuestros sistemas de seguridad, mejoras...debes comunicarla a través del programa Tiquets para que se gestione y garantice la mejora continua de nuestra gestión.

Todas estas políticas de seguridad son de obligado cumplimiento por parte de todo el personal y están incluidas en el Manual de Acogida de la empresa.

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.

Nombre _____

DNI _____

FIRMA _____

(Documento de 13 páginas)