


BUENAS PRÁCTICAS de USO RESPONSABLE de los RECURSOS de PRONET-ISE

Gestión de la Organización

Revisión: 8 Fecha: Junio2022

ÍNDICE

OBJETO DEL DOCUMENTO	3
ALCANCE.....	3
DESARROLLO	3
REFERENCIA NORMATIVA DE LAS BUENAS PRÁCTICAS	4
USO DE MEDIOS INFORMÁTICOS PRIVADOS.....	5
USO ACEPTABLE DE LOS ACTIVOS.....	6
LOS RECURSOS HUMANOS	8
EMPLAZAMIENTO Y PROTECCIÓN DE LOS EQUIPOS	9
SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES.....	10
PROTECCIÓN CONTRA LAS DESCARGAS.....	11
MANIPULACIÓN DE SOPORTES.....	12
INTERCAMBIO DE INFORMACIÓN.....	17
USO DE CONTRASEÑAS.....	19
ORDENADORES PORTÁTILES Y COMUNICACIONES MÓVILES.....	20
FUGAS DE INFORMACIÓN	21
CUMPLIMIENTO DE LOS REQUISITOS LEGALES	22
USO ACEPTABLE DE LOS RECURSOS NATURALES.....	23
CONSUMO ELÉCTRICO	24
PREVENCIÓN DE RIESGOS LABORALES.....	25

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

OBJETO DEL DOCUMENTO

Definir las Buenas prácticas en el uso responsable de los Recursos, humanos, materiales y lógicos de Pronet-ISE en el desarrollo de su actividad conforme a los requisitos estipulados por su Sistema de Gestión Integrado (SGI)

ALCANCE

A todas las actividades desempeñadas por todo el personal de Pronet-ISE bajo el ámbito de su sistema de gestión. Todo el personal debe cumplir estas buenas prácticas y hacer cumplir al personal a su cargo el seguimiento de las mismas. Todo el personal debe de informar cuando tenga conocimiento del personal que no esté cumpliendo algún punto de las mismas, con el fin de poner las medidas necesarias, y dentro del proceso de mejora continua establecido en nuestro sistema de gestión integrado.

Este alcance, según los casos, puede extenderse a los proveedores y terceros que utilicen algún recurso de Pronet-ISE durante el desarrollo de sus actividades.

DESARROLLO


Las buenas prácticas de uso responsable de los recursos de Pronet-ISE del presente documento constituyen un elemento vivo y activo por el cual la Dirección de la organización comunica los requisitos al resto de la misma para operar bajo el condicionado de cada uno de sus epígrafes.

Las actividades bajo el amparo del sistema de gestión se realizan conforme a lo estipulado en el presente documento. Dichas buenas prácticas de uso de los recursos se definen, implementan y operan sin menoscabo de la legislación vigente alineándose siempre con la misma.

Estas buenas prácticas de uso responsable nacen de la aplicación de diversos puntos de las normas del Sistema de gestión Integrado implantado por Pronet-ISE.

REFERENCIA NORMATIVA DE LAS BUENAS PRÁCTICAS

BUENAS PRÁCTICAS	NORMA	APARTADO
Uso de medios Informáticos privados	27001	A.7.2.1
Uso aceptable de los activos	27001	A.8.1.3
Los Recursos Humanos	27001	A.7.1.1 A.7.1.2 A.7.2.1 A.7.2.2 A.7.3.1
Emplazamiento y protección de los equipos	27001	A.9.2.1
Seguridad de los equipos fuera de las instalaciones	27001	A.8.3.3
Protección contra las descargas	27001	A.12.2.1
Manipulación de soportes	27001	A.8.3.1 A.8.3.2 A.8.3.3
Intercambio de información	27001	A.13.2.2 A.13.2.3 A.13.2.4
Uso de las contraseñas	27001	A.9.4.3
Ordenadores portátiles y comunicaciones móviles	27001	A.11.2.6
Fugas de información	27001	A.14.1.1
Cumplimiento de los requisitos legales	27001	A.18.1.1 A.18.1.2
Uso aceptable de los recursos naturales	14001	4.3.1
Consumo eléctrico	14001	4.4.6

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9


USO DE MEDIOS INFORMÁTICOS PRIVADOS

Pronet-ISE tiene personal, tanto en sus oficinas, como en situación de teletrabajo, y provee de los medios informáticos necesarios a sus trabajadores para el desarrollo de su actividad, tanto dentro como fuera de la empresa. Pese a ello ocasionalmente, alguien puede utilizar sus medios personales o privados para el tratamiento de información, relativa al negocio de la empresa.

El personal que utilice medios informáticos personales o privados para el tratamiento de la información, como por ejemplo dispositivos portátiles, ordenadores de uso doméstico, dispositivos de mano, etc., para el tratamiento de la información relativa al negocio de la organización puede introducir nuevas vulnerabilidades, como son la infección por virus de los ficheros tratados, o la incorrecta gestión de los ficheros tratados, por lo que:

- Cuando se procesen ficheros informáticos con información del negocio de Pronet-ISE en un medio personal o privado, éste deberá contar con algún programa antivirus.
- Cuando el fichero se incorpore a la red de Pronet-ISE, deberá ser revisado y verificado por el sistema antivirus de la organización.
- El formato del fichero deberá ser compatible con las versiones de software existentes en Pronet-ISE.
- El usuario deberá mantener las mismas medidas de seguridad que utilizaría en Pronet-ISE: copia de seguridad del fichero, eliminación de versiones obsoletas, etc.
- Una vez incorporado el fichero a la red de Pronet-ISE, deberán de ser eliminadas todas las copias del medio informático privado para evitar su utilización incorrecta, así como para cumplir las disposiciones de confidencialidad de la organización. No se deben mantener ficheros, bajo ninguna circunstancia, propiedad de Pronet-ISE en los dispositivos informáticos privados.

En el caso de utilización de dispositivos terminales móviles privados de forma continuada para el acceso a repositorios de información de Pronet-ISE, éstos figurarán registrados en los entornos de control / gestión de la Organización bajo, al menos, una configuración de dispositivo BYOD (Bring Your Own Device)

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

USO ACEPTABLE DE LOS ACTIVOS

Todos los empleados y terceros que utilicen activos de Pronet-ISE para el tratamiento de la información deberán cumplir las presentes directrices de uso aceptable.

INTERNET

La conexión a Internet es un recurso limitado y además es un componente esencial para el trabajo de Pronet-ISE. En este sentido, las tareas de mantenimiento y soporte son las más críticas porque el uso inadecuado de la conexión a Internet no permite ofrecer un servicio de calidad a nuestros clientes y además aumenta el coste de estas tareas. Por ello, hay que seguir las siguientes normas:

Descargas: Los archivos cuyo tamaño exceda de 50 MB, se descargarán a partir de las 5 de la tarde y asegurando que terminan antes de las 7:45 del día siguiente. Se puede utilizar el lapso de tiempo de las 14:00 a las 14:45 para descargas, consultando previamente con mantenimiento y soporte correspondiente de la línea. Si es muy urgente la descarga del archivo y no puede esperar a la tarde, habrá que consultarlo con Mantenimiento y Sistemas.

Subidas: Los archivos cuyo tamaño exceda de 1 MB y no estemos utilizando ningún gestor FTP, se subirán a partir de las 5 de la tarde. Se puede utilizar el lapso de tiempo de las 14:00 a las 14:45 para subidas sin gestor FTP, consultando previamente con el servicio de soporte. Por ahora, solo subimos archivos a servidores FTP, por lo tanto se recomienda utilizar un gestor FTP limitando la velocidad.

Pronet-ISE no limita el acceso a Internet a los usuarios, pero apela al uso correcto del mismo. La búsqueda de información en Internet debe de ser relativa a actividades de negocio de Pronet-ISE, y se debe de ser vigilante al consumo del ancho de banda de ciertas páginas, que no se deben de usar, como son páginas de vídeos y streaming en línea, intercambio de ficheros, etc.


No está permitido el uso de carpetas de ficheros compartidos en la nube para asuntos privados o particulares como son Dropbox, SkyDrive, etc.

CORREO ELECTRÓNICO

La cuenta de correo electrónico puesta a disposición de cada usuario del dominio @pronet-ise.com es para uso exclusivo de tareas relacionadas con el negocio de Pronet-ISE.

No se deben mandar ficheros adjuntos en los correos internos de la organización si estos ficheros están publicados o pueden ser publicados en el gestor documental. Se deben de enviar enlaces al documento en el gestor documental.

El correo electrónico no es un sistema de almacenamiento de archivos. Siempre que se reciba un correo electrónico con un fichero adjunto que contenga información relativa al negocio de Pronet-ISE, deberá ser almacenado en las carpetas o sistemas de información habilitados a tal efecto.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

Si se reciben correos externos con ficheros adjuntos de mucho peso, deberá indicarse al remitente que según cual sea su capacidad de servidor, puede tener problemas de espacio.

En las cuentas de correo de proveedores externos, que sean utilizadas en el negocio de Pronet-ISE, al existir limitación física de uso por parte del proveedor, deberán de revisarse periódicamente por los usuarios de esas cuentas para garantizar que no falta espacio en los mismos. En caso de necesitarse la eliminación de correos históricos, se guardará una copia del mismo en los lugares habilitados por la organización a tal efecto.

DISPOSITIVOS MÓVILES

El uso de los dispositivos móviles puestos a disposición del personal por Pronet-ISE, es para uso exclusivo de tareas relacionadas con el negocio de Pronet-ISE.

Cuando el dispositivo móvil sea usado fuera de las instalaciones de Pronet-ISE, se deberá proteger mediante el uso de una contraseña o patrón de conexión para evitar su uso por personas ajenas a la organización.

Cuando el usuario se conecte a una red inalámbrica o Wifi fuera de Pronet-ISE, deberá hacerlo sólo de organizaciones que considere seguras. Nunca podrá conectarse a redes abiertas o sin seguridad, para evitar el acceso fraudulento del dispositivo móvil.

Los dispositivos móviles serán controlados en la plataforma Intune gestionada por la Organización. En función de que éstos sean propiedad de la Empresa, o propiedad del Empleado con acceso a recursos / programas de la Organización, la gestión será como “Dispositivo propietario” o “Dispositivo BYOD” (Bring Your Own Device).

La gestión del parque móvil queda definida en el documento “[Pronet IT SIS 01 Guia de Sistemas.docx](#)”

TARJETAS DE ACCESO A LA OFICINA

El uso de tarjetas de acceso a la oficina puesta a disposición del personal por Pronet-ISE, es para uso exclusivo de tareas relacionadas con el negocio de Pronet-ISE.

Cuando la tarjeta se encuentra fuera de las instalaciones de Pronet-ISE, se deberá anonimizar y guardar con la debida cautela para evitar su uso por personas ajenas a la organización.

En caso de pérdida, deberá avisar lo antes posible para su anulación en el sistema.

LOS RECURSOS HUMANOS

INICIO

Pronet-ISE cuando inicia una relación laboral con sus trabajadores provee de los medios materiales e informáticos necesarios a sus trabajadores para el desarrollo de su actividad.

El trabajador cuando recibe estos medios de trabajo es informado de que debe de velar por el buen uso y mantenimiento del mismo, tratándolo con el cuidado necesario, y procurando que su uso y desgaste no vaya más allá del considerado normal en una organización profesional.

Al inicio de la relación laboral el trabajador recibe el Manual de Gestión de la Organización, el Manual de Políticas, el presente documento, y toda aquella documentación relativa a la gestión de su línea de negocio, por lo que quedan definidas sus responsabilidades en lo referente a la confidencialidad, la protección de datos, ética, uso adecuado de los equipos y recursos de la organización, así como las prácticas profesionales que se esperan por la organización.

DURANTE EL EMPLEO

Durante toda la relación laboral que el trabajador debe de velar por el buen uso y mantenimiento de todo el material recibido, tratándolo con el cuidado necesario, y procurando que su uso y deterioro no vaya más allá del considerado normal en una organización profesional.


No podrá utilizar los medios informáticos para el uso o manipulación de información personal que no tenga relación con el negocio de Pronet-ISE.

CESE DEL EMPLEO

Una vez finalizada la relación laboral, el trabajador no podrá utilizar los medios materiales y humanos que se pusieron a su disposición. Si este activo no está en las oficinas de Pronet-ISE, deberá consensuar el calendario para su devolución con su responsable más directo.

Si existiera algún tipo de información en un medio privado o personal, deberá proceder a su devolución y eliminación en el plazo de tiempo más breve posible.

Se le informará de que se le retiran los derechos de acceso. Por razones de confidencialidad y disponibilidad de la información, su cuenta de correo electrónico será direccionada a la persona designada para evitar la pérdida de correos en tránsito, durante un periodo mínimo de 3 meses.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

EMPLAZAMIENTO Y PROTECCIÓN DE LOS EQUIPOS

Durante toda la relación laboral que el trabajador debe de velar por el buen uso y mantenimiento de todo el material recibido, tratándolo con el cuidado necesario, y procurando que su uso y desgaste no vaya más allá del considerado normal en una organización profesional.


No podrá utilizar los medios informáticos para el uso o manipulación de información personal que no tenga relación con el negocio de Pronet-ISE.

Los equipos deben de colocarse en la áreas habilitadas para su conexión a red,, cuidando los aspectos como conexiones, y velando por la información en ellos contenida como se recoge en el Manual de Políticas de Pronet-ISE.

Con el fin de no dañar el material y los equipos informáticos, hay habilitada una zona en las instalaciones de Pronet-ISE, en donde se pueden manipular, calentar y consumir los alimentos. No está permitido el consumo de alimentos fuera del área habilitada para tal fin. Tampoco puede utilizarse en el comedor equipos informáticos si hay personal consumiendo alimentos.

No está permitido fumar en ningún punto de las instalaciones de Pronet-ISE, conforme a la normativa sanitaria vigente.

Pese a que Pronet-ISE vela por el mantenimiento de las condiciones ambientales, tales como temperatura y humedad, si se considera que éstas pueden afectar negativamente a los equipos de tratamiento de la información, deberá reportarse la correspondiente incidencia.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

Como norma general es el B.Owner de cada línea de la empresa la que autoriza el uso de los equipos fuera de nuestras oficinas, generalmente para su uso en las instalaciones de nuestros clientes o clientes potenciales.

Cuando se trate de un ordenador portátil el que se utilice fuera de la oficina se debe llevar en su correspondiente bolsa de transporte adecuada para el portátil que lo protege en los traslados, intentando siempre no separarse del equipo en ningún momento del traslado y respetando siempre, tanto en su uso como en su transporte, las indicaciones establecidas por el fabricante.

Cuando se trate de documentación en soporte lógico o físico, ésta debería de ser la mínima posible, y vigilar que se encuentra siempre disponible y que no puede ser utilizada por un tercero no autorizado, sobre todo durante los periodos de desplazamiento, fuera de las instalaciones de Pronet-ISE o de las instalaciones de los clientes.


Cuando se trate de un equipo de teléfono, se deberá mantener las conversaciones telefónicas en entornos aislados de posibles escuchas por terceros no autorizados. En caso de imposibilidad de conseguir este entorno, se avisará a la otra parte de la imposibilidad de tener la comunicación y se le emplazará a un momento posterior en el que se pueda mantener la misma.

Respecto al trabajo desde fuera de las instalaciones, por defecto están bloqueadas todas las conexiones externas, de cualquier tipo, a la red privada de Pronet ISE a excepción del tráfico del servidor de correo electrónico (puerto SMTP), estando bloqueadas todas las peticiones de entrada mediante un firewall, que se encarga de analizar y filtrar todo el tráfico de entrada y de salida. El acceso a la información contenida en los servidores de Pronet se realizará a través de conexiones gestionadas, controladas y protegidas mediante el sistema VPN implementado en los Firewall de la Organización.

Se ha procedido a estudiar la cobertura de seguros para este tipo de equipos, pero las aseguradoras sólo cubren contingencias de atraco, el resto de vulnerabilidades (extravío, hurto, robo, ...) no son asegurables, por lo que la reducción de este riesgo mediante un seguro no es posible, por lo que el usuario debe de ser responsable y tener en cuenta todas estas contingencias, pero en especial:

- No dejar el equipo sin supervisión en lugares públicos.
- Seguir las instrucciones del fabricante en cuanto a su uso en entornos de trabajo con campos electromagnéticos intensos.

En caso de desaparición por cualquier causa de cualquier equipo o material por parte de un usuario, deberá de informar lo más rápidamente posible a su responsable para poder tomar todas las medidas de protección que se consideren necesarias.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

PROTECCIÓN CONTRA LAS DESCARGAS

Las descargas constituyen el principal elemento de propagación de código malicioso en las organizaciones. Hay que ser muy vigilante en este aspecto, ya que los medios de descarga se desarrollan muy rápidamente, y pueden comprometer seriamente a toda la organización.

No están permitidas las descargas en Pronet-ISE de cualquier software, aplicación fichero o soporte informático de fuentes no autorizadas por un responsable de la organización. Estas medidas son de aplicación tanto en las instalaciones propias de la organización, como en las instalaciones habilitadas en terceros para dar soporte a nuestros clientes, como en las instalaciones de cliente que han sido cedidas por el mismo a Pronet-ISE, para el desarrollo de cualquiera de los servicios que haya contratado el cliente.


La utilización de cualquier software que no respete los derechos de la propiedad intelectual no está permitida.

La utilización de software libre, sea cual sea el tipo de licencia, no está permitida, salvo que haya sido validado por un responsable de la organización o por el habilitador de sistemas de su línea.

Los usuarios, y los equipos que los usuarios tienen asignados, pueden ser auditados por su responsable en cualquier momento para comprobar que se están cumpliendo estas directrices.

Todos los usuarios deben de tener instalado el software antivirus que haya indicado el habilitador de sistemas de su línea, así como de velar de que esta correctamente configurado para su actualización y escaneo de la actividad del equipo que debe de proteger. Deben cumplir las instrucciones que a estos efectos sobre actualización y/o modificación de dicho software le sean remitidas por el habilitador de sistemas de su línea con la mayor celeridad posible.

Los usuarios deben de informar inmediatamente de cualquier descarga o software malicioso que hay podido efectuar con el fin de aislar el equipo afectado y minimizar los efectos que puede tener en toda la organización.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

MANIPULACIÓN DE SOPORTES

SOPORTES EXTRAÍBLES.


Los soportes extraíbles que contengan información de la organización, deben de ser almacenados de acuerdo con lo establecido por la organización, siempre en un armario cerrado, mientras contengan información que pueda afectar a la confidencialidad del mismo.


Los puertos USB, los lectores de CD y DVD y otros soportes como discos duros externos, no se encuentran deshabilitados en Pronet-ISE por razones de negocio, pero es responsabilidad de los usuarios el uso adecuado y conforme a lo establecido en estas directrices.

La información en soporte papel, y que contenga información de carácter confidencial o de uso exclusivo para personal de Pronet-ISE, deben de ser destruidos conforme a los medios que a tal fin tiene establecidos Pronet-ISE. El resto de información en soporte papel, debe de ser depositada en los recipientes que a tal efecto tiene Pronet-ISE para proceder a su reciclado.

Las unidades de disco extraíbles en tránsito deberán estar cifradas con BitLocker independientemente del nivel de confidencialidad de los archivos que almacene.

La contraseña de cifrado y el archivo de recuperación de BitLocker se deberán almacenar en la base de datos de KeePass del rol al que pertenece la persona responsable de la unidad extraíble.

 Cifrado de unidad BitLocker

← → ▾ ↑  > Panel de control > Todos los elementos de Panel de control > Cifrado de unidad BitLocker


Ventana principal del Panel de control


Cifrado de unidad BitLocker

Protege tus archivos y carpetas del acceso no autorizado protegiendo tus unidades con BitLocker.

Unidad de sistema operativo

C: BitLocker desactivado








Unidades de datos fijas


Unidades de datos extraíbles: BitLocker To Go

ESD-USB (D:) BitLocker desactivado





	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

←  Cifrado de unidad BitLocker (D:) ×

Elija cómo desea desbloquear la unidad


Usar una contraseña para desbloquear la unidad
 Las contraseñas deben contener mayúsculas y minúsculas, números, espacios y símbolos.

Escribir la contraseña


Vuelva a escribir la contraseña

Usar la tarjeta inteligente para desbloquear la unidad
 Deberá insertar la tarjeta inteligente. El PIN de la tarjeta inteligente será necesario cuando desbloquee la unidad.

La contraseña debe cumplir los requisitos estándar de complejidad de contraseñas.

←  Cifrado de unidad BitLocker (D:) ×


¿Cómo desea realizar la copia de seguridad de la clave de recuperación?

 El administrador del sistema administra ciertas configuraciones.
 Si olvida la contraseña o pierde la tarjeta inteligente, puede usar la clave de recuperación para acceder a la unidad.


→ Guardar en un archivo

→ Imprimir la clave de recuperación

[¿Cómo puedo encontrar después mi clave de recuperación?](#)

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

×

←  Cifrado de unidad BitLocker (D:)


Elegir qué cantidad de la unidad desea cifrar

Si está instalando BitLocker en una unidad nueva o un equipo nuevo, solo es necesario cifrar la parte de la unidad que se está usando actualmente. BitLocker cifrará los datos nuevos automáticamente conforme los agregue.

Si están instalando BitLocker en un equipo o una unidad que ya se está usando, entonces cifre la unidad completa. Al cifrar la unidad completa, se asegura de que todos los datos están protegidos, incluso datos que haya podido eliminar pero que aún puedan contener información recuperable.

Cifrar solo el espacio en disco utilizado (mejor y más rápido para unidades y equipos nuevos)
 Cifrar la unidad entera (más lento, pero mejor para unidades y PCs que ya se encuentran en uso)

×

←  Cifrado de unidad BitLocker (D:)


Elección del modo de cifrado que se usará

La actualización de Windows 10 (versión 1511) introduce un nuevo modo de cifrado de disco (XTS-AES). Este modo ofrece soporte de integridad adicional, pero no es compatible con las versiones anteriores de Windows.

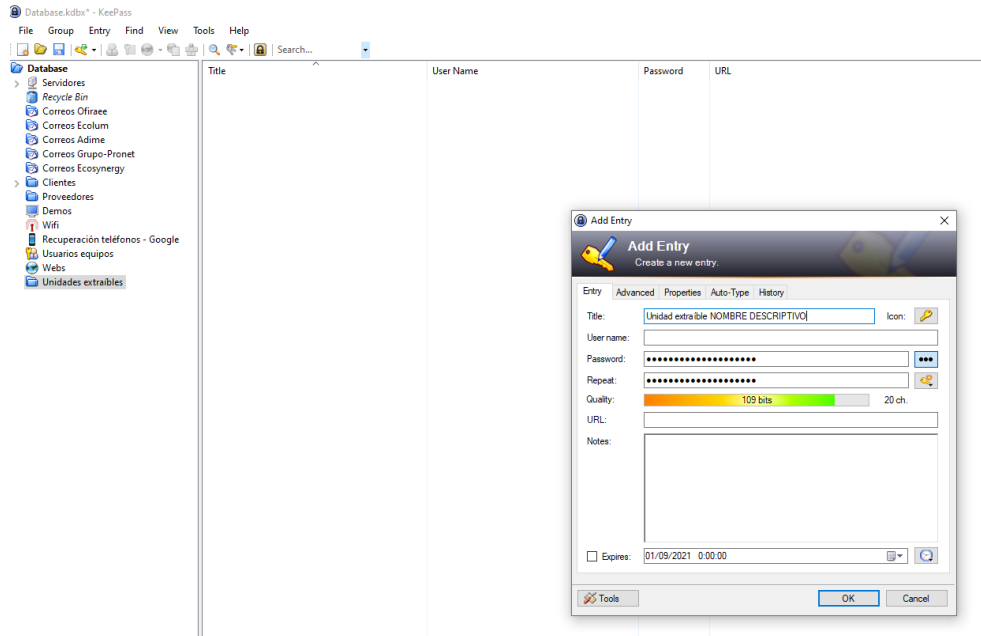
Si se trata de una unidad extraíble que usarás con una versión anterior de Windows, elige el modo Compatible.

Si es una unidad fija o si solo se utilizará en dispositivos con la actualización de Windows 10 (versión 1511) o versiones posteriores, elige el nuevo modo de cifrado.

Modo de cifrado nuevo (recomendado para las unidades fijas en este dispositivo)
 Modo Compatible (recomendado para las unidades que se puedan mover de este dispositivo)

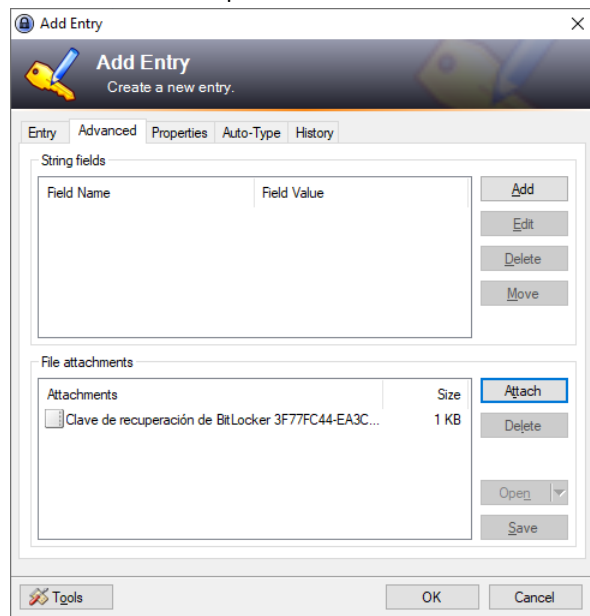
	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS		FECHA	REV.
			Agosto 2023	9

La contraseña y el archivo de recuperación se deberán almacenar en un grupo específico con nombre “Unidades extraíbles” de la siguiente manera:




Donde “NOMBRE DESCRIPTIVO” debe ser el nombre de la persona responsable de la unidad.

El archivo de recuperación se almacenará en los archivos adjuntos del registro que hemos dado de alta:



Este proceso se deberá realizar una vez por dispositivo.


	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

MANIPULACIÓN DE LA INFORMACIÓN

Todo el personal de Pronet-ISE debe de conocer las directrices de clasificación de los documentos, y manipular en consecuencia, la información en función de ese nivel.

Se debe de informar siempre de cualquier sospecha de acceso no autorizado por personal no autorizado a la información que no sea de su competencia.

Dado que existen listas de distribución definidas en la organización, y aunque éstas se revisan periódicamente, se debe de informar por parte del usuario al habilitador de sistemas de cada línea cuando reciba un correo electrónico al que no está autorizado.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9


INTERCAMBIO DE INFORMACIÓN

El intercambio de información en una entidad como Pronet-ISE afecta a todos sus procesos y procedimientos. Este intercambio puede ser a nivel interno (entre personas) o externo, con clientes, proveedores o terceros que no tengan una relación de negocio con Pronet-ISE.

Los intercambios entre líneas deben de realizarse preferentemente en formato electrónico, utilizando preferentemente los medios que la organización pone a disposición de los usuarios, como son las carpetas compartidas a nivel general o departamental o los gestores documentales habilitados en la organización, ya que de todos estos elementos se realiza una copia de seguridad por parte del habilitador de sistemas de la línea y garantiza la disponibilidad de la información en caso de modificación, pérdida o destrucción.

Para intercambios rápidos de mensaje, Pronet-ISE autoriza el uso de una herramienta de mensajería que deberán tener habilitada todos los usuarios y configurada para la conexión automática con el inicio de sesión. No están permitidas otras herramientas de mensajería que la autorizada por Pronet-ISE, así como tampoco está autorizado el uso de la herramienta de mensajería para actividades ajenas al negocio de Pronet-ISE

Los intercambios con personal externo, deben de realizarse preferentemente en formato electrónico, a través del correo electrónico, y se deberá guardar el elemento enviado como prueba y registro de su envío. Caso de ser necesario incorporar ficheros en este correo, éstos estarán en formato no modificable por el tercero (PDF o similar), salvo que las circunstancias del proyecto determinen otro formato. Todos los mensajes deben de ser enviados utilizando la cuenta del dominio @pronet-ise.com que el usuario tiene asignada. No está autorizado el intercambio de información con otras cuentas de correo externas a Pronet-ISE, salvo autorización del responsable y una vez confirmado con el habilitador de sistemas de la línea la existencia de alguna incidencia en el servidor de correo de Pronet-ISE. Todos los mensajes deben de contener la firma del usuario que lo envía, así como el aviso legal que haya sido habilitado por Pronet-ISE.


	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

Caso de intercambios con personal externo que precisen de un soporte físico, sólo pueden utilizarse aquellos transportistas que hayan sido autorizados por administración, para envíos, y debería identificarse previamente con los terceros externos cual va a ser el transportista utilizado, para recepciones. En ambos casos el usuario deberá asegurarse del adecuado embalaje (avisando al tercero si es necesario) del soporte a enviar o recibir, conforme a las especificaciones del fabricante, y que soporte los posibles daños como son golpes, calor, humedad, campos electromagnéticos, etc. Si se recibe un paquete con signos de manipulación o forzado externo, se deberá presentar reclamación al transportista y notificarlo al tercero responsable del envío para tomar las medidas que se consideren necesarias.

Si la sensibilidad de la información lo aconseja, se deberá realizar el envío en varios paquetes y soportes para evitar la posibilidad de acceso completo.

El intercambio de información puede realizarse diferentes soportes. A lo largo de los diferentes puntos de este documento de buenas prácticas de uso responsable de los recursos, se han definido aspectos como:

- El manipulado de información
- La detección y protección de código malicioso.
- La protección de la información sensible.
- El uso de comunicaciones dentro y fuera de las instalaciones.
- La impresión de documentos.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

USO DE CONTRASEÑAS

Las contraseñas de acceso, tanto al dominio de Pronet-ISE, como a los proyectos relacionados con clientes y proveedores, son responsabilidad de cada uno de los trabajadores de Pronet-ISE. En el documento de confidencialidad firmado por cada uno de los trabajadores, se definen las responsabilidades del uso de la cuenta del dominio de Pronet-ISE y su obligación de no facilitar la misma a nadie.

Las contraseñas que gestionan los usuarios deben de ser cambiadas en cuanto se tenga constancia o se tengan sospechas de que puede haber sido conocida o utilizada por terceros no autorizados.

Se recomienda a todo el personal que:

- a) Mantenga la confidencialidad de las contraseñas.
- b) Evite el guardar un registro de las contraseñas, en papel o pos-it, en un fichero de software o en un dispositivo manual. No deben de estar visibles bajo ninguna circunstancia.
- c) Seleccione contraseñas de calidad con una mínima longitud pero suficiente para:
 - 1) Ser fáciles de recordar.
 - 2) Que no estén basadas en algo que alguien más pueda adivinar fácilmente u obtener usando la información relativa a la persona, por ejemplo nombres, números de teléfono, fechas de nacimiento etc.
 - 3) No ser vulnerables a ataques de diccionario, es decir, que no consistan en palabras incluidas en diccionarios.
 - 4) No contengan caracteres consecutivos, idénticos, todos numéricos o todos alfanuméricos.
- d) Cambie las contraseñas a intervalos regulares y evitar la reutilización o utilización cíclica de las antiguas contraseñas.
- e) Cambie las contraseñas provisionales en la primera entrada.
- f) No use la misma contraseña para propósitos profesionales que para no profesionales.

Con Independencia de las recomendaciones contenidas en este documento, Pronet-ISE gestiona a través de sus sistemas informáticos los requisitos mínimos de complejidad y seguridad de las contraseñas de acceso, incluyendo la política de autenticación multifactor.

ORDENADORES PORTÁTILES Y COMUNICACIONES MÓVILES


Los ordenadores portátiles y teléfonos móviles son puestos a disposición del personal de Pronet-ISE para el desarrollo de su actividad. Los trabajadores de Pronet-ISE conocen la “Política de Ordenadores Portátiles y Comunicaciones Móviles” de la organización.

Ordenadores Portátiles.

- Sólo deben usarse en entornos de trabajo que cumplan las especificaciones del fabricante en cuanto a temperatura, presencia de polvo y vibraciones.
- Deben transportarse con los elementos de transporte necesarios para evitar posibles daños.
- Deben de estar siempre protegidos con contraseña, que se modificará cuando se considere que pueda haber sido conocida por personal ajeno a Pronet-ISE.
- Con el fin de alargar la vida de las baterías, la recarga de las mismas sólo deberá realizarse cuando salga el aviso de carga baja y con el dispositivo homologado por el fabricante para su carga.
- Cuando se abandonen las instalaciones externas de Pronet-ISE se verificará que se recoge todo el material adicional necesario como cargador, ratones y demás periféricos para evitar su no posible utilización por falta de estos componentes.
- Debe de asegurarse la actualización continua del software Antivirus y parches anti-vulnerabilidades del sistema operativo de los ordenadores.

Teléfonos Móviles

- Sólo deben usarse en entornos de trabajo que cumplan las especificaciones del fabricante en cuanto a temperatura, presencia de polvo y vibraciones.
- Deben transportarse con los cuidados necesarios para evitar posibles daños.
- Deben de estar siempre protegidos con contraseña /PIN que se modificará cuando se considere que pueda haber sido conocida por personal ajeno a Pronet-ISE.
- Con el fin de alargar la vida de las baterías, la recarga de las mismas sólo deberá realizarse cuando salga el aviso de carga baja y con el dispositivo homologado por el fabricante para su carga.
- Cuando se abandonen las instalaciones externas de Pronet-ISE se verificará que se recoge todo el material adicional necesario, como cargadores y auriculares, para evitar su no posible utilización por falta de estos componentes.
- El consumo del teléfono móvil es responsabilidad del usuario. Las llamadas realizadas desde los mismos deben de obedecer a razones profesionales dentro de la actividad de Pronet-ISE.
- La empresa gestionará la configuración del parque de telefonía móvil mediante utilidades de control MDM.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

FUGAS DE INFORMACIÓN

La información es uno de los principales activos de Pronet-ISE. Deben de evitarse las situaciones que puedan provocar la fuga de información accidental dentro de nuestra organización.


Todos los trabajadores han firmado el documento de confidencialidad en el trato de la información, pero deben de ser especialmente vigilantes en la gestión de los soportes que la contienen.

Soporte físico:

- Sólo deben de imprimirse aquella información estrictamente necesaria.
- Una vez utilizada, y según su nivel de clasificación, debe de ser depositada en los contenedores habitados, rota parcialmente, o en la destructora. No se deben de tirar nunca folios completos al contenedor, ya que aunque sea información de bajo nivel, su lectura es muy fácil por personal ajeno a la organización.
- Los documentos que salgan de las instalaciones de Pronet-ISE deberán de custodiarse con la diligencia necesaria hasta su entrega a cliente o proveedor, o retorno a las oficinas de Pronet-ISE.

Soporte lógico:

- Solo pueden usarse los dispositivos (CD, DVD, llaves USB, discos duros externos, dispositivos móviles) que sean propiedad de Pronet-ISE. NO puede usarse cualquier tipo de dispositivo personal o particular.
- Sólo usarse para aquella información estrictamente necesaria.
- Es responsabilidad del usuario gestionar estos ficheros de forma que siempre esté disponible en Pronet-ISE la versión actualizada del mismo. En caso de actualización en las instalaciones.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

CUMPLIMIENTO DE LOS REQUISITOS LEGALES

El objetivo es evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad por parte del personal de Pronet-ISE.

Derechos de Propiedad Intelectual.

Sólo pueden instalarse, en cualquiera de los dispositivos que Pronet-ISE pone a disposición del personal, software homologado por el habilitador de Sistemas y que no infrinja los derechos de autor. No está permitida la instalación de Software que incumpla el anterior punto y que no proceda de fuentes de confianza. No está permitida la instalación de software libre que no haya debidamente homologado.

Cada usuario es responsable del software que tiene instalado en los equipos puestos a su disposición, por lo que deberá de justificar la presencia de aquel instalado sin las presentes directrices.

Se deben cumplir siempre las condiciones contractuales y de uso de los programas de terceros instalados en equipos de Pronet-ISE. En caso de duda de las mismas, deben de consultarse con el habilitador de sistemas.


En el caso de lectura, uso o consulta de información pública o disponible en Internet, todos los trabajadores no deben de duplicar, convertir a otro formato ni extraer de grabaciones comerciales (de vídeo o audio) más de lo que permita la ley de derechos de autor. Tampoco pueden copiar parcial o totalmente libros, artículos, informes u otros documentos más allá de lo que permita la ley de derechos de autor.

Uso indebido de recursos de tratamiento de la información.

Los medios que Pronet-ISE ponen a disposición de su personal son exclusivamente para el desarrollo de la actividad profesional que le haya sido encomendada, dentro del negocio de Pronet-ISE.

Todo el personal de Pronet-ISE ha sido informado de cuales son sus responsabilidades en el ámbito de la organización, cuales son los niveles de autorización de acceso a la información, y han firmado el documento de confidencialidad con Pronet-ISE. Este documento y su alcance debe de tenerse permanentemente en cuenta en el desarrollo de la actividad de todo el personal, con el fin de cumplir las disposiciones legales que sean de aplicación.


El personal debe de informar a su responsable cuando tenga conocimiento del no cumplimiento de estos dos apartados por parte de otra persona, ya sea un tercero o personal propio de la empresa, con el fin de implementar las medidas necesarias para evitar que la situación se reproduzca en el futuro.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

USO ACEPTABLE DE LOS RECURSOS NATURALES

Los recursos naturales son escasos, tienen un coste económico para la organización, y un coste medioambiental para el planeta. Se apela a toda la organización a un uso aceptable de los recursos, tanto de la empresa como de los particulares, velando por:

- Papel: utilizar el estrictamente necesario, imprimiendo los documentos por ambas caras, y reciclando el mismo una vez finalizada la vida útil del mismo.
- El resto de los consumibles (bolígrafos, cuadernos, pos-it, ...) debe de realizarse también de forma responsable para reducir el impacto medioambiental de los residuos que generan.
- Realizar la separación de residuos habilitada por la empresa. En los depósitos de papel no depositar otro tipo de residuo. El residuo orgánico debe de ser depositado en el recipiente de la cocina para evitar los malos olores en la oficina por su descomposición.
- Reciclar todos aquellos envases en los que su etiquetado lo indique. Utilizar las instalaciones que a tal fin pone a disposición la empresa.
- Depositar el tóner de las impresoras en el área habilitada a tal fin. Dar aviso a administración si el depósito está a punto de llenarse.
- Reutilizar todos los aparatos eléctricos y electrónicos, ya sea total o parcialmente, con el fin de reducir los residuos generados. Hay que asegurarse del no funcionamiento del dispositivo antes de considerarlo, a todos los efectos, residuo de la empresa.
- Depositar los residuos de aparatos eléctricos y electrónicos en el área habilitada por la empresa para tal fin. Asegurarse con el habilitador de sistemas del correcto tratamiento de los dispositivos que puedan contener información.
- Utilizar el lavavajillas de la cocina de forma responsable, llenarlo siguiendo las indicaciones, y ponerlo en funcionamiento sólo cuando esté lleno.
- Realizar un consumo responsable del agua en la cocina, en los sanitarios y en los lavabos.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

CONSUMO ELÉCTRICO

Uno de los principales consumos que realiza Pronet-ISE es el consumo eléctrico, debido principalmente a la naturaleza tecnológica de su actividad. Para racionalizar su uso, el personal de Pronet-ISE velará por:

- Mantener conectados a la red los dispositivos imprescindibles para el desarrollo de su actividad.
- Al finalizar la jornada laboral, se asegurará que el equipo informático queda apagado, así como las pantallas y periféricos que puedan estar conectados.
- Informar de cualquier circunstancia que afecte al buen funcionamiento de cualquier aparato eléctrico o electrónico para su reparación lo antes posible.

No está permitida la conexión a la red eléctrica de Pronet-ISE de aparatos eléctricos y electrónicos particulares o personales de forma permanente. La conexión de aparatos eléctricos y electrónicos de clientes y proveedores deberá de estar supervisada por personal de Pronet-ISE.


Respecto a la climatización, todas las peticiones de cambio deben de ser gestionadas a través de administración, único interlocutor válido para solicitar estos cambios.

Respecto a la iluminación de las instalaciones se tendrá en cuenta que

Las zonas de alumbrado se gestionarán con la llegada y partida del primer y último usuario de cada zona respectivamente, de forma que:

- El primer trabajador en llegar a las instalaciones de Pronet-ISE encenderá única y exclusivamente el alumbrado de su zona.
- El primer trabajador que llegué del resto de zonas, accionará su alumbrado.
- El último trabajador que abandone una zona procederá al apagado del alumbrado de su zona.
- El último trabajador que abandone las instalaciones de Pronet-ISE procederá al apago del alumbrado de su zona y verificará el apagado completo del alumbrado de la instalación.

La gestión del consumo eléctrico del CPD de Pronet-ISE es responsabilidad del habilitador de sistemas.

	BUENAS PRÁCTICAS DE USO RESPONSABLE DE LOS RECURSOS	FECHA	REV.
		Agosto 2023	9

PREVENCIÓN DE RIESGOS LABORALES

Pronet consciente de la salud laboral de sus trabajadores, ha contratado un Servicio de Prevención Ajeno, en todas las modalidades: seguridad, higiene, ergonomía y vigilancia de la salud.

Adicionalmente se recomienda el cumplimiento de las siguientes actividades

- Pronet pone a disposición de los trabajadores medios de protección y/o reducción del riesgo laboral y recomienda su uso responsable a lo largo de la jornada laboral.
- Pronet pone a disposición de sus trabajadores un reconocimiento médico, establecido con la periodicidad recomendada por los profesionales médicos, donde se le dará información referente a su salud laboral y unas pautas de vida saludable.
- Pronet pone a disposición de los trabajadores guías y consejos sobre prácticas adecuadas en el puesto de trabajo para su uso y consulta, así como la documentación generada por el Servicio de Prevención Ajeno.
- Se recomienda a los trabajadores mantener estas diligencias en los traslados desde su vivienda al puesto de trabajo, tanto en medios propios como en transporte público.
- Pronet pone a disposición de los nuevos trabajadores un curso de formación sobre seguridad y salud en oficinas.

Recordar a los trabajadores que existe, además de la representación de los trabajadores, un trabajador designado para la gestión de la actividad preventiva, que podrá recoger todas las recomendaciones y sugerencias por parte del personal de la organización.