ecoembes

CÓDIGO DE BUENAS PRÁCTICAS

EN SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

2025

www.ecoembes.com/es

ecoembes

Índice

ecoembes

1.Introducción

1.1. Política de Seguridad

La Dirección está comprometida con la seguridad de la información y, por ello, **ha aprobado la Política de Seguridad de la Información**, conforme a la norma ISO/IEC 27001. En esta Política se establecen los principios y directrices para garantizar la confidencialidad, integridad y disponibilidad de la información.

Todas las áreas de la organización son **responsables de promover, comunicar y facilitar el cumplimiento de esta Política**, dotando de los recursos humanos, técnicos y económicos necesarios para su aplicación efectiva.

Esta Política **es de obligado conocimiento y cumplimiento para todo el personal** de Ecoembes, incluyendo empleados, dirección, proveedores y colaboradores externos que, directa o indirectamente, accedan, traten o gestionen información de la organización.

El contenido íntegro de la política está **disponible para su consulta en el siguiente enlace:** [enlace a la política].

1.2. Gestión de la Seguridad de la Información

- **La información es uno de los activos más importantes de la compañía.** Las actividades de Ecoembes dependen en gran medida de la calidad de la información que se gestiona y de los sistemas que las soportan.
- Las acciones de seguridad y gestión de la información son necesarias para mantener los niveles de **Confidencialidad, Integridad y Disponibilidad** de dicha información de manera proporcionada al riesgo.
- La **Seguridad de la Información afecta a todos los trabajadores, tanto internos como externos**, ya sean: empleados propios, contratistas, terceros, personal de outsourcing, ETT, personal en prácticas, etc.
- La **sensibilización, concienciación y formación** del personal que maneje o pueda manejar información de la compañía garantiza la consecución de los niveles de seguridad y protección marcados por la Dirección de la compañía.

1.3. Código de Buenas Prácticas

- El objetivo de este documento es divulgar un conjunto de buenas prácticas entre los trabajadores y colaboradores de Ecoembes para sensibilizar, concienciar y contribuir a **alcanzar los niveles de seguridad que ha establecido la compañía.**
- En el marco de la seguridad de la Información, **el Reglamento General de Protección de Datos (RGPD)** contribuye a garantizar el tratamiento adecuado de la información relativa a datos personales, como se verá a lo largo del documento.
- Ecoembes establece que el contenido de este Código de Buenas Prácticas es de **obligado conocimiento y cumplimiento** para cualquier persona que haga uso de los Sistemas de Información internos, **pudiéndose, en caso de que se detecten infracciones sobre el mismo, iniciar un proceso sancionador interno** por parte de la compañía.

1.4. Clasificación de la información

Toda la información creada, almacenada o transmitida a través de los Sistemas de Información de la compañía, poseerá uno de los siguientes niveles:

- **Sin restricción:** Información de uso público, por lo tanto, puede ser utilizada libremente tanto interna como externamente.
- **Información Privada:** Información sensible para Ecoembes y que requiere de medidas y controles de protección frente a la revelación, alteración o eliminación no autorizada de la misma. En función de la sensibilidad de dicha información se definirá como:
    - **Confidencial:** Información que no está disponible para el uso público ya que tiene una naturaleza más sensible. Por ejemplo, datos de negocio de Ecoembes o de clientes o datos de carácter personal.
    - **Muy Confidencial:** Información de negocio o de clientes o datos de carácter personal que se consideran más sensibles o que contengan una mayor cantidad de información, y que su robo o difusión puede poner en peligro procesos de la organización o la imagen de Ecoembes.
    - **Restringido:** Información privada relacionada con asuntos de Ecoembes muy sensible, la cual solo puede ser conocida y accesible por unos pocos individuos dentro de Ecoembes, es decir por el conjunto de Gerentes o el Comité de Dirección.

Para obtener más información sobre el uso del sistema de etiquetado y clasificación de documentos y correos electrónicos, así como sobre las medidas de seguridad aplicables a la documentación en papel, puede contactar con la Oficina de Seguridad a través del correo electrónico seguridad@ecoembes.com o consultar las guías disponibles en el Portal DWP.

ecoembes

1.5. Etiquetado de la información

El etiquetado de la información se realizará de acuerdo con su clasificación:

■ **Sin restricción:**
No se considera necesario el etiquetado de la información clasificada como "Sin restricción", dado que no requiere medidas especiales de protección.

■**Confidencial:**
- **Uso externo editable:** tanto los empleados como los usuarios externos a la organización pueden editar, leer, imprimir, copiar, reenviar y capturar/compartir pantalla en videoconferencias.
- **Uso externo solo lectura:** los empleados y las personas externas pueden leer, imprimir y reenviar el contenido, pero no pueden editar, copiar ni capturar/compartir pantalla en videoconferencias.
- **Uso interno editable:** solo los empleados pueden leer, editar, copiar, imprimir, reenviar el contenido y capturar/compartir pantalla en videoconferencias.
- **Uso interno solo lectura:** solo los empleados pueden leer, imprimir y reenviar el contenido, pero no pueden editar, copiar ni capturar/compartir pantalla en videoconferencias.

Además, todas estas etiquetas añaden una cabecera al correo/documento indicando "Contenido confidencial".

■**Muy Confidencial:**
- **Uso externo solo lectura:** solo los empleados y las personas externas pueden leer el contenido, pero no pueden editar, copiar, imprimir, reenviar el contenido ni capturar/compartir pantalla en videoconferencias.
- **Uso interno solo lectura:** solo los empleados pueden leer el contenido, pero no pueden editar, copiar, imprimir, reenviar el contenido ni capturar/compartir pantalla en videoconferencias

Además, todas estas etiquetas añaden una cabecera al correo/documento indicando "Contenido muy confidencial".

■**Restringido:**
- **Comité Dirección solo lectura:** solo el Comité de Dirección puede leer el contenido, pero no pueden editar, copiar, imprimir, reenviar el contenido ni capturar/compartir pantalla en videoconferencias.
- **Gerentes solo lectura:** solo los Gerentes de Ecoembes pueden leer el contenido, pero no pueden editar, copiar, imprimir, reenviar el contenido ni capturar/compartir pantalla en videoconferencias.

Además, todas estas etiquetas añaden una cabecera al correo/documento indicando "Contenido restringido".

2. Responsabilidades de las personas

2.1. Conceptos generales

2.2. Trabajo fuera de las instalaciones de Ecoembes

2.3. Monitorización de los Sistemas de Información y Recursos Tecnológicos

2.1. Conceptos generales

- Un Sistema de Información de la compañía es cualquier dispositivo corporativo en el cual se procesa o almacena información, esto incluye cualquier elemento de usuario final como PC's, portátiles, tabletas o smartphone.
- Se establece como requisito obligatorio para toda persona con cuenta en los Sistemas de Información de la compañía el **conocer, aceptar y cumplir el presente Código de Buenas Prácticas,** constituyendo o formando parte de la Política de Seguridad en vigor.
- Cada persona es responsable del uso que realiza sobre la información que trata y gestiona, tanto dentro, como fuera de las instalaciones de la compañía.
- **Los Sistemas de Información deben utilizarse solo para fines de negocio.** Cualquier otra finalidad deberá ser aprobada por la Dirección.
- Si la persona detecta que un activo de información crítico ha sufrido una pérdida de confidencialidad, integridad o cualquier otra anomalía que pueda afectar a la seguridad de la información se debe considerar un **Incidente de Seguridad**, y como tal, notificar a la Oficina de Seguridad. La comunicación de los incidentes de seguridad, siempre que técnicamente sea posible, se hará mediante un correo electrónico a la dirección de correo electrónico **seguridad@ecoembes.com.**
- **Queda prohibido extraer, para uso propio o para su cesión a terceros, documentación, software o cualquier tipo de información corporativa confidencial o sensible en formato papel o electrónico**, con la excepción de asuntos relacionados con los Proceso de Negocio de la compañía o cuando esta acción haya sido expresamente autorizada por la Dirección. Esta prohibición incluye, entre otros, la extracción mediante dispositivos USB, transferencia a través de plataformas de Internet, así como el envío de la citada información a direcciones de correo electrónico personales.

En casos de que se evidencie intencionalidad en la pérdida, corrupción o divulgación de datos, se procederá a retirar los accesos concedidos a la persona.

ecoembes

2.2. Trabajo fuera de las instalaciones de Ecoembes

- El acceso a internet debe realizarse únicamente a través de **redes seguras o previamente autorizadas**, quedando prohibido el uso de redes Wi-Fi públicas. (cafeterías, hoteles, transporte, etc.).
- En caso de **no** disponer de una **red segura, se utiliza la red de datos móviles** (4G/5G).
- Las **redes Wi-Fi personales** deben contar, como mínimo, con cifrado WPA2 y tener desactivada la opción WPS.
- **No** se utilizarán **identificadores** de red (SSID) **que revelen información personal.**
- Las **contraseñas por defecto del router deben ser modificadas**, utilizando credenciales robustas tanto para el acceso como para la administración del dispositivo.
- El **router** debe mantenerse **actualizado y con los servicios innecesarios deshabilitados.**
- Se deben utilizar exclusivamente **dispositivos y herramientas corporativas.**
- **Evitar el acceso a los dispositivos por parte de terceros**, especialmente en entornos domésticos.
- La **salida** de **portátiles y móviles** está **autorizada, debiendo garantizarse su custodia y protección** frente a accesos no autorizados, pérdida o sustracción.
- **Cuando se trabaje en lugares públicos** como trenes o aviones se debe **impedir la visibilidad del equipo y su información en pantalla**.
- Las **reuniones virtuales** deben programarse con el **número exacto de participantes y cerrarse una vez iniciadas.**
- Para **grabar las sesiones**, los participantes tienen que dar su aprobación y en la sesión se mostrará a todos los usuarios un indicador visual y sonoro de que se está produciendo la grabación.
- **No compartir nunca públicamente el enlace a la reunión**, ni su ID, ni el PIN de moderador o invitado.

ecoembes

2.3. Monitorización de los Sistemas de Información y Recursos Tecnológicos

- Con la aprobación la Dirección, se encuentran implementados sistemas que realizan **monitorización continua del uso que hacen empleados y personal externo de los Sistemas de Información,** de los recursos de la plataforma tecnológica que se les ha asignado, y del tratamiento y transmisión de la información que se gestiona desde los mismos, dejando evidencias y registros de las acciones llevadas a cabo por las personas.
- Así mismo, las monitorizaciones implementarán políticas para prevenir y/o justificar operaciones que en cada momento la Dirección determine que puedan ser susceptibles de un riesgo para el negocio, tales como extracción de información sensible fuera del SharePoint o OneDrive Corporativo, posibles conflictos o incumplimiento de la Política de Seguridad o de la Política de Privacidad marcada por el Reglamento de Protección de Datos Personales (RGPD), un uso de los Sistemas Corporativos dudoso o para actividades del ámbito personal.
- La Dirección de Tecnología y Digital es la responsable de la definición, gestión y custodia, de los registros de auditoría generados en los sistemas.
- Se realizarán **periódicamente auditorías de carácter total o parcial,** con el objeto de verificar el grado de cumplimiento, a la vez que se comprobará la eficacia de las herramientas de monitorización implantadas en cada momento.
- Recordar, una vez más, el **principio de corresponsabilidad:** el personal debe preservar la seguridad de los activos que Ecoembes pone a su disposición, en consonancia con las políticas y procedimientos vigentes en cada momento. Igualmente, todo el personal debe utilizar los activos estrictamente para el desempeño de las actividades propias de su puesto de trabajo y funciones asignadas.

3. Seguridad física

3.1. Control de acceso físico

Acceso a las instalaciones

- Todo el personal de Ecoembes dispone de una **tarjeta de acceso personal e intransferible,** siendo su responsabilidad mantenerla y conservarla, así como notificar, lo antes posible, su pérdida o deterioro.
- Los empleados que posean tarjeta de **acceso al parking** actuarán del mismo modo descrito en el punto anterior.

Visitas

- El acceso de visitantes y personal externo, requerirá siempre de un **registro y la obtención de una identificación temporal** antes de ingresar en las instalaciones.
- Durante el tiempo que el visitante permanezca en las oficinas corporativas, deberá estar acompañado en todo momento por la **persona responsable** de Ecoembes que esté a su cargo.
- En caso de **emergencia o evacuación**, la persona responsable, deberá encargarse de los visitantes o externos que se encuentren a su cargo.

Áreas de acceso restringido

- El acceso a los lugares restringidos, que estarán debidamente marcados o indicados, **estarán estrictamente controlados y limitados a determinados empleados** de la compañía. En caso de ser necesario el acceso de empleados no autorizados o incluso personal externo, estos estarán en todo momento acompañados por personal de la compañía que sí tenga autorizado el acceso.
- Existirá un **registro de entradas y salidas** en entornos restringidos para empleados, visitantes o terceros.
- El uso de **equipos fotográficos, video, audio u otro tipo de grabación está prohibido**, a menos que se cuente con autorización previa.

3.2. Política de mesas limpias

Para reducir los riesgos de acceso no autorizado, pérdida o daño de la información se han establecido las siguientes directrices:

- **Al finalizar la jornada o al ausentarse del puesto de trabajo por un periodo de tiempo prolongado**, la persona deberá recoger los papeles y almacenarlos en los lugares destinados para tal fin, de forma que el lugar de trabajo quede despejado.
- Todo documento en papel, que contenga información que se pueda considerar como confidencial, muy confidencial o restringida, deberá guardarse en **armarios o cajoneras bajo llave.**
- **No** se deberán **anotarse** contraseñas, palabras clave, o cualquier otro tipo de código en post-it, paneles, pizarras o cualquier otro sitio a modo de nota.
- **Se limita el consumo de alimentos y bebidas** en zonas donde se encuentren equipos o activos de información, con el fin de prevenir daños accidentales
- Cualquier **situación** relacionada con información que represente un **riesgo** debe ser **reportada a la Oficina de Seguridad**.
- **No está permitido el uso de soportes** digitales de información, como llaves de memoria USB, discos duros externos, etc., **salvo autorización previa y expresa**. En caso de autorización, la persona propietaria o asignada será responsable de cualquier acción o tratamiento de información realizado mediante dichos dispositivos.
- Los soportes digitales que contengan información, que se pueda considerar como confidencial, muy confidencial o restringida, deberán guardarse en **armarios o cajoneras bajo llave.**

3.3. Impresoras, fotocopiadoras y escáneres

- El sistema de multifuncionales está configurado para **registrar la actividad** que cada persona hace de los mismos.
- **Las impresoras disponen de un mecanismo de autenticación**, de tal manera que los remitentes son los únicos que pueden obtener sus impresiones.
- **Imprime sólo** documentos con **información necesaria** para las tareas de tu trabajo.
- Cuando la documentación impresa haya dejado de tener utilidad, deposítala en los contenedores de papel. Si el documento contiene información sensible, entonces destrúyelo **utilizando las destructoras de papel, o deposítala en los contenedores específicos** habilitados para el reciclaje bajo procedimientos seguros este tipo de documentación.

3.4. Equipos desatendidos

- Los equipos **se bloquean de manera automática** una vez transcurrido un tiempo de inactividad definido.
- En cualquier caso, debes **bloquear de manera proactiva el acceso lógico al mismo cada vez que abandones tu puesto de trabajo.**
- En el caso de detectar algún equipo desatendido sin bloquear, deberíamos bloquearlo nosotros mismos y contactar con su propietario, animándole a que proceda a hacerlo.
  - **Al término de la jornada laboral, deberá apagar su estación.** Si no fuera posible la dejara bloqueada al igual que en el supuesto anterior.
  - **No apuntar la contraseña de acceso,** ni la dejará en las proximidades o pegada en la estación de trabajo.
- Debemos intentar que los **equipos portátiles** permanezcan siempre con nosotros, y fuera del horario laboral o cuando abandonamos la oficina, si dejamos el equipo en la misma este deberá **guardarse en armario o cajonera con llave.**

3.5. Revisiones

La **Oficina de Seguridad o la persona en quien se delegue, podrán realizar revisiones** para comprobar el cumplimiento de los siguientes aspectos:

- **Revisión de equipos portátiles y dispositivos móviles**, comprobando que fuera del horario laboral no se queden solos en los puestos de trabajo o salas de reunión sin ningún tipo de salvaguarda. Igualmente, durante el horario laboral, se podrá comprobar que no se dejen equipos desatendidos donde no está activada la pantalla de bloqueo
- **Revisión de Puestos de Trabajo**, con el objeto de identificar información sensible o que contenga datos de carácter personal sin que esta esté custodiada.
- **Revisión de armarios y cajoneras**, identificando si permanecen abiertos fuera del horario laboral, y en los mismos existe documentación sensible o con datos personales.
- **Revisión de las zonas de reprografía**, para identificar si existe documentación que no ha sido recogida.

Tras dicha revisión, se podrá realizar un **informe en el que se indiquen los resultados encontrados,** los cuales serán trasladados a los diferentes responsables de áreas.

ecoembes

4. Seguridad Lógica

4.1. Contraseñas de acceso a los sistemas

- Para acceder a los Sistemas de Información Corporativos es necesario identificarse y autenticarse correctamente en el mismo.
- Las **contraseñas son personales e intransferibles.** Será responsabilidad de cada persona mantenerla como tal.
- Las contraseñas deben ser **renovadas periódicamente**, siendo 90 días el plazo máximo marcado por la organización.
- La cuenta y/o contraseña utilizada en Ecoembes, no debe ser la misma que se emplee en **Sistemas de Información ajenos a la compañía.**
- Está limitada a 4 intentos de inicio de sesión fallidos antes de bloquear temporalmente la cuenta.
- Evita almacenar las contraseñas en texto plano
- Es obligatorio utilizar la autenticación **multifactor** (MFA) cuando el sistema lo solicite. El sistema empleará algoritmos para determinar cunado debe solicitar el segundo factor y así validar tu acceso. En el Portal DWP podrás encontrar guías de configuración y uso de MFA y restablecimiento de contraseña.

La política de contraseñas actual exige los siguientes requerimientos:

Longitud mínima: 12 caracteres

La contraseña debe incluir al menos tres de los siguientes tipos de caracteres:

123 Contener un número

ABC Contener una letra mayúscula

abc Contener una letra minúscula

@$ Contener un caracter especial

4.2. Gestión de archivos y copias de seguridad

- Cada persona es responsable de la información que almacena en su propio equipo de trabajo (disco duro del propio equipo). **Cualquier información almacenada en local no se incluirá en las copias de seguridad.**
- Recuerda que es responsabilidad de cada uno de nosotros que toda documentación importante, útil para la organización, o para tu propia actividad laboral debes siempre guardarla o subirla a los Servicios Corporativos dispuestos para ello de MS Office 365, ya que de estos si se realizan copias de respaldo.
- **No debes almacenar archivos personales en los Servicios corporativos de MS Office 365 o en tu propio equipo de trabajo.** La información almacenada debe ser exclusivamente profesional.
- **Cualquier información almacenada en tu equipo o en los Servicios Corporativos podrá ser accedida por la organización** para fines de vigilancia, control laboral o asegurar el adecuado uso de los recursos, durante la relación laboral y a su finalización.

La información almacenada en los equipos y servidores de la compañía debe ser exclusivamente profesional

4.3. Gestión de soportes electrónicos

- Los **puertos USB** de los dispositivos corporativos están **deshabilitados por defecto.** Solo podrán habilitarse de forma excepcional y con autorización previa y expresa.
- Las personas son **responsables del cuidado y uso adecuado** de los soportes electrónicos.
- En caso de que tenga acceso a información sensible en un soporte físico, **deberá almacenarla de forma segura o devolverla** al Dpto. de Plataforma Digital y Ciberseguridad para su almacenaje centralizado cuando ya no la necesite.
- Las personas **no deben compartir los dispositivos** asignados con otras personas, a menos que se cuenta con una autorización para ello.
- Para prevenir posibles pérdidas de información, **los soportes no deben almacenarse cerca de fuentes magnéticas**, solares y térmicas.
- Las personas no están autorizadas, salvo por orden expresa, a **realizar copias de seguridad en dispositivos** y soportes externos.
- Aquellos soportes que hayan almacenado información considerada sensible, es recomendable que antes de ser reutilizado, se realice un proceso de borrado con procedimientos seguros de forma que los datos que habían contenido no sean recuperables de ninguna manera. En estos casos, podéis realizar una solicitud al CAS.
- En lo relativo a la limpieza de documentación de los discos duros internos de los equipos cuando estos se dejan de utilizar, el equipo de soporte técnico llevará a cabo un borrado bajo procedimientos seguros de forma que se elimine toda la información que en algún momento se guardó y se eliminen las posibilidades de recuperación avanzadas por terceros.

ecoembes

4.4. Instalación y uso de software

- **La instalación de software no autorizado por la compañía puede causar conflictos** y/o efectos no deseados en el puesto de trabajo o en los Sistemas Corporativos. Además, puede conllevar **sanciones económicas y daños en la imagen de Ecoembes.**

Queda prohibido instalar programas sin una autorización expresa

- La instalación de software deberá ser realizada por el Equipo de Soporte o en cualquier caso bajo el conocimiento, autorización y provisión de la Dirección de Tecnología y Digital.
- En caso de necesitar un software o herramientas informáticas que no se encuentre disponible en la compañía, debe solicitarse a la Oficina de Seguridad.

Uso correcto y proporcionado de los programas y aplicaciones

- **El Dpto. de Plataforma Digital y Ciberseguridad es el responsable de inspeccionar el software en los equipos personales y desinstalar o eliminar cualquier programa que no haya sido previamente autorizado o se considere susceptible de ser un riesgo de seguridad para los Sistemas de Información de la compañía.** Del mismo modo, la persona responderá ante cualquier instalación no autorizada, que podrá quedar registrada como incidente de seguridad.
- Hacer un uso correcto del software y aplicaciones que Ecoembes proporciona al personal, entendiendo por buen uso las actividades propias del negocio y sin acciones u operaciones malintencionadas.

ecoembes

4.5. Gestión de información en la nube

- Está prohibido el uso de herramientas como WeTransfer, Dropbox, Mega, whatsapp, etc., para el intercambio de documentación corporativa, a menos que esta acción sea autorizada por la Oficina de Seguridad. **Las únicas herramientas autorizadas por defecto para almacenar e intercambiar información son las herramientas de nuestro sistema de Microsoft 365 (Teams, SharePoint, o OneDrive).**
- Nuevamente indicar, que la información almacenada o compartida desde nuestros sistemas en nube debe ser estrictamente profesional.
- Se recomienda realizar una correcta identificación de los documentos y la aplicación del sistema de etiquetado con cifrado para así evitar posibles futuras difusiones de información a personas no autorizadas cuando compartimos información.
- Ecoembes únicamente realizará y garantizará la copia y recuperación de datos que estén almacenados o hayan sido gestionados a través de nuestro sistema de **Microsoft 365.**
- Todos los movimientos de almacenamiento, modificación, copia, descarga y eliminación de la información en la nube, será supervisada, registrados y guardada como evidencia con el fin de asegurar un buen uso de esta.

5. Seguridad en los dispositivos móviles

5.1. Protección de equipos portátiles

5.2. Seguridad de móviles y tabletas electrónicas

5.3. Seguridad en dispositivos

5.1. Protección de quipos portátiles

- Es responsabilidad de cada empleado la **custodia, protección física y salvaguarda de la información que su equipo portátil contenga.**
- Fuera del puesto de trabajo, si no estamos utilizando el equipo portátil, debe **guardarse bajo llave o fuera del alcance de terceros.**
- La **pantalla del dispositivo deberá bloquearse** tras un tiempo de inactividad. Este bloqueo se encontrará protegido por, al menos, un código PIN de acceso. Asimismo, no se podrá acceder a ningún tipo de funcionalidad y/o información del dispositivo mientras el terminal se encuentre bloqueado.
- En los desplazamientos y viajes, el equipo **no debe facturarse como equipaje** y **debe mantenerse en todo momento bajo nuestro control.** En los hoteles, siempre que sea posible, es conveniente dejarlo en la caja de seguridad.
- En caso de **robo, extravío o acceso** no autorizado, se debe comunicarlo antes posible a la Oficina de Seguridad .

No debemos conectar nuestroequipo portátil a redes WIFI públicas, redes WIFI sin contraseña o redes WIFI que cuenten con autenticación WEP. De manera general, a cualquier red WIFI de fuentes desconocidas o que no consideremos suficientemente seguras.

- Activar itinerancia, se recomienda la compartición de red de datos desde el móvil antes de conectarse a Internet a través redes desconocida.
- Velar por la información almacenada en el dispositivo: la información propiedad de Ecoembes debe usarse de manera responsable y exclusivamente para fines profesionales de consulta con carácter confidencial.
- Realizar descargas de archivos sólo si se tiene conocimiento de lo que es: Las descargas indiscriminadas o sin autorización son uno de los orígenes más usuales de infección por código malicioso.
- No descargar código o software no confiable: Es necesario asegurar la confiabilidad del sitio desde el cual se descargan las aplicaciones, utilizando siempre los repositorios oficiales.
- Eliminar los datos de carácter confidencial y privados: los dispositivos móviles serán sometidos a técnicas de borrado seguro por la Oficina de Seguridad.

5.2. Seguridad de móviles y tabletas electrónicas

Si dispones de Smartphone corporativo, dispones de aplicaciones para instalar, pero muchas no son verificadas por terceros de confianza. Es importante ser muy cauto a la hora de instalarlas y usarlas. Al igual que ocurre con los PC, ejecutar o utilizar programas y archivos provenientes de fuentes dudosas puede suponer un riesgo de seguridad.

Dos de cada tres personas que utilizan Smartphone leen su correo electrónico en este tipo de dispositivos

- **Protege tu Smartphone como si de tu cartera se tratase, su contenido tiene valor.** Los cibercriminales transformar sus ataques en dinero debido al volumen de información que pueden obtener de los dispositivos móviles de las personas.
  - Encaso de pérdida o robo, comunícalo inmediatamente.
  - Realice las actualizaciones automáticas del dispositivo o recomendadas por Ecoembes.
  - Deshabilite las conexiones NCF, Bluetooth, WIFI, en caso de no usarlas.
  - Desactive su ubicación si no se usa.
  - Deshabilite los permisos por defecto.
  - Cierre sesión en aquellas páginas o aplicaciones cuando deje de visitarlas y/o utilizarlas.

El 90% de los usuarios de Smartphone en España almacena fotos, el 80% documentos personales y el 76% contactos de amigos y compañeros de trabajo.

- **Conectar dispositivos a la red supone un riesgo para la información que almacena y gestiona con ellos.** Evite las redes públicas y las conexiones de red gratuitas: no tienen los controles de seguridad adecuados y cualquiera podría acceder a sus datos.
- **Realiza copias de seguridad** regulares de los datos importantes almacenados en tu dispositivo móvil o Tablet.

Para leer y contestar los correos, utilizar la red móvil del dispositivo, nunca wifi gratuitas o de fuentes desconocidas.

5.3. Seguridad en dispositivos

Ecoembes dispone de herramientas, las cuales monitorizan y protegen los dispositivos de posibles amenazas como navegación segura, instalación de apps de dudosa reputación, trafico cifrado, etc.

- DLP con el fin de monitorizar las posibles fugas de información
- AV/EDR para proporcionar una capa de seguridad a la hora de análisis de posibles ficheros maliciosos que abrimos o almacenamos desde el dispositivo al igual que los patrones de comportamiento sospechoso.
- Navegación segura con filtrado de sitios webs sospechosos o de contenidos catalogados como impropios
- Los dispositivos móviles corporativos, tendrán instalados aplicaciones que protegen al dispositivo, y ayuda a analizar y bloquear amenazas. Monitoriza configuraciones del sistema operativo, el comportamiento de aplicaciones instaladas en el mismo, conexiones a redes. Asimismo, recopila información, que será analizada para identificar comportamientos sospechosos.

Es recomendable estar atentos a las alertas y notificaciones, cualquier evento o incidencia debería ser comunicado a la Oficina de Seguridad.

Más allá de estas herramientas, recordar, en cualquier caso, que será responsabilidad de la persona el correcto uso que hace de los dispositivos que la organización le ha asignado.

ecoembes

6. Virus y *software* malicioso

6.1. Tipología

6.2. Medidas de prevención

6.3. Medidas de actuación

Cualquier programa o código malicioso que ejecute acciones dañinas y no deseadas en un sistema informático. Invade y deshabilita ordenadores, sistemas informáticos, dispositivos móviles, etc. asumiendo su control parcial. No daña el hardware de los sistemas o el equipo de red, pero puede robar, cifrar o borrar datos, y espiar con el objetivo final de sacar beneficio económico ilícito.

6. Tipología

Para entender las amenazas que puedan afectar a la información y a los sistemas de la compañía es importante conocer los tipos de malware que existen y que pueden afectarnos:

Virus:

Programas maliciosos que "infectan" otros archivos para modificarlo o dañarlo. Se reproducen incrustando su código malicioso en un archivo limpio que se convierte en portador del virus, extendiéndose por todo el sistema informático e infectando a archivos con el propio código malicioso.

Gusanos:

Son un código similar al virus, buscan replicarse a sí mismos dentro de una misma red de ordenadores, provocando daños en datos y archivos, incluso llegando a destruirlos.

Troyanos:

Es uno de los tipos de malware más peligrosos. Es un programa aparentemente útil que pasa inadvertido. Se instaura en el sistema al ejecutarse y los atacantes (ocultos tras el troyano), tienen acceso no autorizado al dispositivo infectado, consiguiendo robar todo tipo de información (credenciales, financiera, redes sociales, datos personales, etc.) o instalando nuevos virus.

Adware:

Software de publicidad de distintos productos o servicios que recopilan información sobre gustos y visitas o redirigen las búsquedas a sitios webs publicitarios. El usuario percibe este malware de un modo intrusivo y molesto cuando utiliza un explorador.

Spyware:

Es un software que recopila toda la información que hay en un ordenador o en un dispositivo electrónico y se la envía al dueño del spyware. El usuario no se da cuenta de ello.

6. Tipología

Ransomware:

Simula un secuestro digital: bloquea el acceso a los usuarios a sus propios dispositivos y cifra sus archivos para posteriormente forzarle a pagar un rescate. Las nuevas divisas electrónicas, como los bitcoins, "favorecen" estos ataques ya que exigen un pago rápido y provechoso de difícil seguimiento.
Este tipo de código malicioso se obtiene a través de mercados ilegales en línea, y defenderse de ellos es muy complejo. Por eso, cuida la descarga de archivos y tu navegación por internet.

Registrador de pulsaciones de teclas:

Es un software basado en la grabación de todas las pulsaciones de teclas que realiza el usuario. Almacena toda la información recopilada y se la envía al atacante, quien busca información confidencial: contraseñas, nombres de usuario, números de tarjetas de crédito, etc.

Botnets:

Red construida por muchos equipos informáticos secuestrados por malware, controlados por el atacante quien envía nuevos virus, roba información o realiza ataques de denegación de servicio distribuido (DDoS). Constituyen una de las principales amenazas en la actualidad.

ecoembes

6.2. Medidas de prevención

- **No instalar software no autorizado** ni ilegal /sin licencia.
- Disponer del equipo siempre **actualizado**, y sistemas **Antimalware**(antivirus).
- No hacer clic en posibles **pop-ups** durante la navegación con contenido desconocido.
- No conectar **USB** no controlados, en caso de que estén autorizados los puertos USB del dispositivo, e informar al equipo de seguridad.
- No utilizar cuentas de **correo corporativas** para darse de alta en páginas web no relacionadas con el trabajo.
- Use el botón de ***"Informar sobre correo de phishing"*** para reportar posibles casos.
- No responda a correos **SPAM.**
- Inspeccione los **enlaces** que vaya a visitar.
- Revisar que el programa antimalware de sus puestos de usuario como de sus dispositivos estén actualizados; ejecute un análisis que permita identificar el malware y que gestione los pasos necesarios para eliminarlo.
- Realiza un formateo completo de la unidad afectada; perderás aquella documentación que no tengas guardada en tu última copia de seguridad o en la nube, pero evitarás perder más información y, por consiguiente, reducirás la probabilidad de que te puedan chantajear.

ecoembes

Si detectas un virus deberás:

6.3. Medidas de actuación

1. Desconectar el equipo de la red a la que se encuentre conectado (cable o WiFi).
2. Comunicarlo de manera inmediata a la Oficina de Seguridad o en su defecto al Equipo de Soporte Microinformático.
3. Salir del programa/aplicación en el que estás trabajando sin guardar los cambios, pero no apagar en ningún caso el PC.
4. No utilizar el equipo o dispositivo hasta que se te indique lo contrario.

En la notificación, utiliza los canales establecidos e intenta ser lo más preciso posible, explicando el origen, las acciones realizadas y cualquier tipo de información de utilidad.

7. Ingeniería Social

¿Qué sabemos de ingeniería social?

La Ingeniería social es una técnica que emplean los ciberdelincuentes para ganarse la confianza del usuario y conseguir así que haga algo bajo su manipulación y engaño, como puede ser ejecutar un programa malicioso, facilitar sus claves privadas o comprar en sitios web fraudulentos.

Los ataques de ingeniería social manipulan a las personas para que compartan información que no deberían compartir, descarguen software que no deberían descargar, visiten sitios web que no deberían visitar, envíen dinero a delincuentes o cometan otros errores que comprometan su seguridad personal u organizacional.

7.2. Tipos de ataques

7.2.1 El phishing (o suplantación de identidad)

Es una modalidad de estafa que tiene por objetivo ganarse la confianza de sus víctimas, haciéndose pasar por otra persona, empresa o servicio de confianza, para manipularles y engañarles y así obtener sus datos personales, credenciales, cuentas bancarias, números de tarjetas, contraseñas, etc. Vamos a verlo con detalle.

Tipos de phishing:

- **Correos electrónicos** masivos de phishing se envían a millones de destinatarios a la vez. Parecen ser enviados por una empresa u organización grande y conocida, como un banco nacional o mundial, un gran minorista en línea, un popular proveedor de pagos en línea, etc., y hacen una petición genérica como «tenemos problemas para procesar su compra, actualice su información de crédito».
- **QR Phishing:** Quishing es esencialmente un ataque de phishing que utiliza inteligentemente códigos QR para engañar a los usuarios para que visiten sitios web maliciosos. Cuando un usuario escanea un código QR malicioso, su navegador va al sitio web indicado por el código QR.
- **Spear phishing** tiene como objetivo una persona concreta, normalmente alguien con acceso privilegiado a la información de los usuarios, a la red informática o a los fondos de la empresa. Un estafador investigará al objetivo, a menudo utilizando información que se encuentra en LinkedIn, Facebook u otras redes sociales para crear un mensaje que parezca proceder de alguien que el objetivo conoce y en quien confía o que haga referencia a situaciones con las que el objetivo está familiarizado.
- **Whale phishing** es un ataque de suplantación de identidad rápida que se dirige a una persona de alto perfil, como un CEO o un conocido cargo político.
- **Phishing de voz o vishing**, es el phishing que se realiza a través de llamadas telefónicas. Las personas suelen experimentar vishing en forma de llamadas grabadas amenazantes.
- **El phishing por SMS, o smishing**, es el phishing a través de un mensaje de texto.
- **La suplantación de identidad en los motores de búsqueda** implica que los piratas informáticos creen sitios web maliciosos que ocupan un lugar destacado en los resultados de búsqueda para los términos de búsqueda más populares.
- **Angler phishing** es una variante del phishing que consiste en la suplantación de identidad mediante cuentas falsas en las redes sociales, las cuales se hacen pasar por las cuentas oficiales de los equipos de atención al cliente o servicio de atención al cliente de empresas de confianza.

7.2. Tipos de ataques

7.2.1 Baiting

Mediante un señuelo se atrae (sin doble sentido) a las víctimas para que, consciente o inconscientemente, faciliten información confidencial o descarguen código malicioso, tentándolas con una oferta valiosa o incluso un objeto de valor.

7.2.3 Tailgating

En el tailgating, también llamado «piggybacking», una persona no autorizada sigue de cerca a una persona autorizada hasta una zona que contiene información sensible o activos valiosos.

7.2.4 Pretextar

En el pretexto, el actor de la amenaza crea una situación falsa para la víctima y se hace pasar por la persona adecuada para resolverla.

7.2.5 Quid pro quo

En una estafa quid pro quo, los piratas informáticos ofrecen un bien o servicio deseable a cambio de la información confidencial de la víctima.

7.2.6 Scareware

También considerado una forma de malware, el scareware es un software que utiliza el miedo para manipular a las personas para que compartan información confidencial o descarguen malware.

7.2.7 Ataque de abrevadero

Derivado de la frase "alguien envenenó el abrevadero": inyectan código malicioso en una página web legítima frecuentada por sus objetivos.

ecoembes

7.3. Medidas preventivas

Cuidado con la información que proporcionas, en dónde, cuándo y a quién.

■Evita facilitar datos confidenciales a través de una llamada telefónica;
■Recuerda que la sensación de urgencia es sinónimo de fraude.
■Ignora enlaces que te generen dudas desde un correo electrónico, SMS o cualquier otro canal.
■Revisa que el mensaje, el emisor y los enlaces no contengan erratas o formas de expresión extrañas.
■Sospecha de mensajes que generen una sensación de urgencia o euforia.
■Antes de acceder a un enlace, pasa el cursor del ratón por encima de él para ver a dónde te redirige.
■Recuerda: las empresas legítimas no te solicitarán datos personales por email, SMS o por teléfono sin previo aviso
■Si crees que estás siendo víctima de un ataque, contacta con la Oficina de Seguridad (seguridad@ecoembes.com) lo antes posible.
■Sospecha de mensajes que generen una sensación de urgencia o euforia.
■Haz uso del doble factor de autenticación siempre que sea posible.
■¿Qué debes hacer si detectas alguna actividad u operación sospechosas?¿Y si has sido víctima? Cambiar todas tus contraseñas de inmediato.

8. Uso de internet y del correo electrónico

8.1. Utilización y acceso a internet

8.2. Utilización del correo electrónico

8.1. Utilización y acceso a internet

La persona debe entender que el navegador es una herramienta muy compleja capaz de manejar numerosas tecnologías y que, al igual que cualquier otro programa, está sujeta a vulnerabilidades y a gran variedad de ataques. Por ello, se deben tomar una serie de medidas para evitar un posible ataque por esta vía.

- **Utiliza internet de manera responsable** y razonable para proteger la información y los sistemas de la compañía.
- Evita acceder a **sitios web con contenido inapropiado** o de ética cuestionable.
- Mantente **alerta** ante banners, ventanas emergentes con enlaces, promociones "engañosas",etc.
- Asegurarse que el navegador, así como plugins, extensiones y cualquier otro elemento que utilice, están **actualizados** correctamente. Un navegador actualizado evitará gran parte de los problemas relacionados con posibles exploits.
- **Deshabilitar o eliminar las extensiones en desuso** ya que la persona esta aumentando su superficie de exposición de forma innecesaria.
- Se recomienda **no utilizar el almacenamiento de credenciales** ya que se si el equipo se ve comprometido es relativamente sencillo acceder a dichas credenciales. Además, si el equipo es compartido de forma no segura, es trivial acceder a las credenciales.

Es recomendable que no se almacene las sesiones asociadas a servicios web que manejen información sensible o crítica en el equipo y se cierre las mismas una vez que finalice la navegación.

- **No deben instalarse plugins/extensiones** desde sitios no oficiales (aquellos no relacionados con el del propio sitio del desarrollador).
- **No debe hacerse clic en enlaces sospechosos**; por ejemplo, los recibidos por medio del correo electrónico.

8.2. Utilización del correo electrónico

Actualmente el correo electrónico sigue siendo una de las herramientas más utilizadas por cualquier entorno corporativo para el intercambio de información. A pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros, el correo electrónico parece seguir siendo la herramienta predilecta de muchas empresas y personas. No es de extrañar, por tanto, que los atacantes traten de utilizar este medio para tratar de infectar y comprometer equipos.

Como personal de Ecoembes, podemos tomar una serie de medidas para protegernos de posibles ataques:

- Identificar correos electrónicos dañinos con algunas de las siguientes recomendaciones:
  - **Correos con patrón fuera de lo común**
  - **Verificación del remitente**
  - **Comprobación de los ficheros descargados**
  - **Actualización del sistema operativo y de las aplicaciones**
  - **Macros en los documentos ofimáticos**

- Debe **informarse inmediatamente a la Oficina de Seguridad** en el caso de recibir un correo sospechoso (las faltas de ortografía suelen ser una señal bastante reveladora).
- Si el contenido del correo electrónico que se desea enviar es sensible se recomienda el uso de **herramientas adicionales para garantizar la integridad y confidencialidad del mismo**. Por ejemplo, herramientas como GPG o plugins para clientes de correo como Enigmail.
- En el caso de utilizar la versión web para acceder al correo electrónico **no deben de almacenarse las credenciales en el propio navegador** ya que éstas pueden ser recuperadas en caso de infección por determinados tipos de malware.
- Si se va a enviar un mensaje a varias personas u se quiere evitar que los destinatarios puedan ver el resto de direcciones, **se debe utilizar la función de copia oculta (CCO).**

9. Redes sociales corporativas

9.1. Perfil de ecoembes

9.2. Riesgos presentes

9.3. Guía de utilización

ecoembes

Nuestras redes sociales

9.1. Perfil de Ecoembes

- Ecoembes es una empresa con un marcado perfil público en redes sociales, transmitiendo nuestros valores, visión y misión del reciclaje.
- Como empleado de nuestra compañía queremos hacerte partícipe de esta visión y que en la medida de lo posible demuestres **tu implicación con nuestros valores.**

9.2. Riesgos presentes

La utilización de redes sociales corporativas tiene su parte positiva a la vez que ciertos inconvenientes. **Permitir al personal de Ecoembes la utilización de estos servicios es política de la compañía.** Por este motivo, queremos destacar, y que comprendas, **las consecuencias de una mala utilización de nuestras redes sociales:**

Utilización de las redes sociales con precaución

- Falta de control sobre el contenido
- Secuestro de Marca
- Daños a la imagen por representación negativa
- Desvelo de información confidencial
- Utilización de ancho de banda
- Bajada de productividad
- Exposición a virus, malware

9.3. Guía de utilización

La utilización de las redes sociales corporativas requiere de unas ciertas **nociones básicas de seguridad y normas de actuación.** Por favor, cuando utilices redes sociales corporativas, hazlo **SIEMPRE** bajo las siguientes **instrucciones de obligado cumplimiento:**

ecoembes

Instrucciones de obligado cumplimiento

- **Nunca publiques datos de carácter personal** o información sensible para la compañía
- **Nunca utilices el logotipo de Ecoembes,** sus eslóganes o marcas registradas, o alguna de sus marcas identificativas en un sitio web
- Sólo los colaboradores autorizados que han sido oficialmente designados por Ecoembes pueden hablar en su nombre
- Debes dar por hecho que lo que escribes puede ser de dominio público
- La información puede escapar por completo a tu control una vez que ha sido publicada
- Como empleado de Ecoembes, tus actividades en los medios sociales influyen en tu imagen y también en la de la organización. **Evita** por tanto **unirte a grupos de medios sociales que no reflejan nuestros valores como organización.**
- Ecoembes espera de ti que **utilices tu criterio y buen juicio** en todas las situaciones y especialmente en tus relaciones con personas desconocidas. **Eres responsable de lo que publicas y de tu conducta en los medios online.** Recuerda que, en determinadas situaciones, podrías tener que responder personalmente por tus acciones, así que debes meditar siempre antes de publicar contenido en Internet.
- Con la excepción de redes de contactos profesionales, jamás debes utilizar la dirección de correo corporativa como referencia de contacto al suscribirte o registrarte en servicio alguno, a menos que dicho servicio sea necesario por motivos genuinamente profesionales o esté asociado con tu actividad de trabajo.
- Eres responsable de todo lo que publicas, incluso si lo borras posteriormente. Una vez publicado un comentario o una foto en un medio social, puede ser fácilmente compartido por otra persona, guardado en otros sitios, o capturado por software de terceros. **Debes tener siempre en cuenta que cualquier cosa que publicas en Internet escapa de manera efectiva a tu control** una vez publicada.

10. Uso de la IA

La Inteligencia Artificial, conocida como IA por sus siglas, son sistemas informáticos diseñados para imitar y replicar algunas capacidades cognitivas humanas, como el aprendizaje, la percepción, el razonamiento y la toma de decisiones. Esta tecnología se basa en algoritmos complejos y utiliza grandes cantidades de datos para realizar tareas específicas.

A continuación, se detallan algunas recomendaciones para evitar riesgos en la privacidad:

- **Se consciente de que información compartes.** No compartas datos e información corporativa sensible o de carácter personal en Servicios de IA públicos, ya que podemos perder el control y la trazabilidad de los mismos al ser almacenados en sistemas externos a Ecoembes y poder ser utilizados en su beneficio.
- **Verifica la información.** Es esencial tener un equilibrio entre las soluciones de IA, y la supervisión humana. Cuando la IA nos proporcione una respuestas o resultados, debemos asegurarnos de ella ya que puede estar desactualizada, sesgada o errónea.
- **Verifica sus fuentes**: No tomes la IA como una fuente absoluta de verdad. Siempre verifica los hechos consultando diferentes fuentes confiables. A pesar de la automatización y las capacidades avanzadas que la IA aporta, el factor humano sigue siendo insustituible.
- **Cuidado con el sesgo:** Recuerda que la IA puede estar sesgadas según la información con la que se haya entrenado. Especialmente el aprendizaje profundo, puede funcionar como una «caja negra». Esto significa que, aunque un modelo pueda predecir o clasificar con alta precisión, a menudo es difícil entender cómo llegó a una decisión particular ya que lo que se le ha enseñado previamente puede ser erróneo.
- **Lee la política de datos:** Es importante que antes de aceptar las políticas de privacidad y términos de uso, se lean estas para saber cómo la aplicación va a manejar la información que introducimos ya que cada aplicación puede tener unas políticas distintas.

11. Normativa de Protección de Datos de Carácter Personal

11.1. Reglamento de protección de datos

11.2. Principios de Protección de Datos de Carácter Personal

ecoembes

11.1. Reglamento de protección de datos

- El Reglamento General de Protección de Datos tiene como principal objetivo potenciar el respeto por las libertades y derechos fundamentales de las personas, y adapta la gestión de los datos personales a los nuevos entornos digitales y al uso de los mismos.
- El **incumplimiento** de los requisitos derivados del RGPD puede dar lugar a sanciones y un impacto negativo en la imagen y reputación de Ecoembes.
- El **RGPD se ciñe a los datos de carácter personal (DCP)**, esto es, cualquier información concerniente a personas físicas identificadas o identificables, no a personas jurídicas.

La política de privacidad se encuentra publicada en nuestra web corporativa.

- Tus datos personales se conservarán mientras se mantenga en vigor tu relación laboral con Ecoembes y durante el plazo de conservación legalmente establecido a tal efecto. Tus derechos ARCOPOL vienen recogidos en la política de privacidad.

Información de contacto del Delegado de Protección de Datos: oficinadeprivacidad@ecoembes.com

- La Agencia Española de Protección de Datos (AEPD)es el organismo oficial encargado de velar por el cumplimiento de la ley. Para más información puedes consultar su página web: **www.agpd.es.**

11.2. Principios de protección de datos de carácter personal

1.Objetivo

El objetivo de estos Principios de Protección de Datos de Carácter Personal, a partir de ahora principios, es definir las líneas de actuación, que conformarán la estrategia corporativa en materia de privacidad y que conduzcan a la elaboración de unas directrices claras y concisas que definan las pautas a seguir en el tratamiento de datos de carácter personal.

La formulación de estos principios se sustenta en los siguientes pilares claves para lograr la protección de la información de Ecoembes:

- Los datos de carácter personal deben ser protegidos conforme a su **susceptibilidad, valor y criticidad.**
- Todos los empleados y terceros colaboradores de Ecoembes, tienen la **responsabilidad de protegerlos datos de carácter personal que se les ha confiado.**
- La protección de los datos de carácter personal permite el desarrollo del negocio y las medidas de protección deben diseñarse conforme a una evaluación del riesgo.

2. Ámbito de aplicación

Estos principios incluyen la estrategia y responsabilidades aplicables a todas las personas, procesos y tecnologías existentes en Ecoembes, tanto en sus oficinas centrales, delegaciones, Circular Lab, así como **cualquier otra ubicación donde se genere, procese, almacene y/o elimine datos de carácter personal.**

ecoembes

11.2. Principios de protección de datos de carácter personal

3. Definiciones

Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

GDPR (General Data Protection Regulation): Reglamento europeo de protección de datos de obligado cumplimiento.

4. Responsabilidad

La aplicación y cumplimiento de los Principios de Protección de Datos de Carácter Personal **es responsabilidad de todos los empleados, y terceros de Ecoembes,** independientemente de quien sea el responsable de dichos tratamientos.

Consecuentemente, los empleados y todos aquellos terceros subcontratados son copartícipes de dicha responsabilidad, debiendo trabajar, desde la posición que ocupen e independientemente de la responsabilidad que explícitamente se les asigne, hacia la consecución de una adecuada protección de los datos.

Los empleados de Ecoembes, así como el personal subcontratado o colaboradores externos, **deberán conocer, asumir y cumplir los principios, normativas y procedimientos de privacidad vigentes**, estando obligados a mantener el secreto profesional y la confidencialidad de los datos manejados en su entorno laboral y debiendo **comunicar**, con carácter de urgencia y según los procedimientos establecidos, **las posibles incidencias o problemas que se detecten.**

ecoembes

11.2. Principios de protección de datos de carácter personal

5. Declaración

Por expreso deseo de Ecoembes, se establecen los presentes Principios de Protección de Datos de Carácter Personal de acuerdo a los requisitos legales vigentes:

- **RGPD: Reglamento General de Protección de Datos** - UE 2016/679, sobre protección de datos de las personas físicas y la circulación de los mismos.
- **LOPD-GDD: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales:** aprobado en Consejo de Ministros en 18 de octubre de 2018

Todos los empleados, colaboradores y terceras partes tienen la responsabilidad de asegurar que, tanto ellos como cualquier otra persona o entidad a su cargo, conocen, respetan y hacen respetar estos principios.

12. Sanciones disciplinarias

1. Faltas y sanciones de los trabajadores

Según lo que recoge el Estatuto de los Trabajadores y el convenio colectivo al que se adscribe Ecoembes, se establece un **marco normativo que regula las acciones disciplinarias** que pueden aplicarse a los empleados en caso de incumplimiento de sus obligaciones laborales.

El **Estatuto de los Trabajadores proporciona las bases legales** que afectan a cualquier trabajador, definiendo conductas que pudieran ser consideradas como faltas leves, graves o muy graves, así como los procedimientos que deben seguirse para su imposición.

De manera complementaria, **el convenio colectivo** complementa la normativa comentada con especificaciones que se adaptan a las particularidades de Ecoembes y el sector en el cual opera.

13. Comunicación de incidentes y debilidades

Comunicación de incidentes

Debes ser consciente que, dentro de tus responsabilidades, si detectas escenarios que estén poniendo en riesgo la seguridad de la información motivado por un ataque, fallos del sistema, o situaciones de malas praxis, debes reportar las mismas tan pronto como sea posible.

Este tipo de incidencias, debes notificarlo, explicando los hechos detectados a la Oficina de Seguridad enviando un correo a seguridad@ecoembes.com

Comunicación de vulnerabilidades

Igualmente, si detectas situaciones potenciales, vulnerabilidades, o algún tipo de sospecha que ponga en riesgo la seguridad de la información, también debes informar a la Oficina de Seguridad, indicando siempre que te sea posible la siguiente información:

- Áreas afectadas/s
- Proceso o Actividad
- Breve descripción de la vulnerabilidad
- Evidencias (capturas de pantalla/adjuntos)

Código Ético de Ecoembes

Adicionalmente, Ecoembes dispone de un Código Ético y de un canal ético que se encuentra abierto a todos los miembros de la organización y terceros relacionados con Ecoembes. El contenido del Código Ético se puede consultar en el siguiente enlace: https://www.ecoembes.com/landing/codigo-etico/

14. ANEXO 1

Aceptación de la Política de Seguridad la Información y el Código de Buenas Prácticas en Seguridad de la información y Protección de Datos

Aceptación de la Política de Seguridad de la Información y el Código de Buenas Prácticas en Seguridad de la información y Protección de Datos

Declaro haber leído la "Política de Seguridad de la Información" y el "Código de Buenas Prácticas en Seguridad de la información y Protección de Datos", que se encuentran a disposición de todas las personas en la Intranet y acepto el cumplimiento de las normas de seguridad y protección de datos expresadas en estos documentos, asumiendo las consecuencias que en caso contrario pudieran derivarse por Ley. En especial declaro haber comprendido:

- **La Política de Seguridad de la Información.**
- **El uso aceptable de la información y los activos asociados.**
- **Las normas relativas al Reglamento General de Protección de Datos.**
- **Las Obligaciones en materia de protección de datos de carácter personal.**

Obligaciones legales en materia de Protección de Datos de Carácter Personal: Para el desarrollo de las funciones que le son inherentes a su puesto de trabajo, el/la trabajador/a puede tener acceso a datos de carácter personal de cuyo tratamiento es responsable la Empresa, así como al resto de información generada por la actividad de la misma. Tales tratamientos están afectos al cumplimiento de las disposiciones contenidas en las normativas aplicables en materia de protección de datos tanto a nivel nacional como a nivel europeo. De conformidad con lo previsto en dichas normativas el/la trabajador/a se compromete a guardar plena confidencialidad sobre los datos de carácter personal incluidos en los ficheros de la Empresa, incluso una vez finalizada la relación laboral entre las partes. El/la trabajador/a se compromete igualmente a cumplir y hacer cumplir las medidas de seguridad aplicadas a los sistemas de tratamiento, así como a respetar las normas expuestas en el presente Código de Buenas Prácticas de uso de los sistemas informáticos que el responsable del tratamiento ponga a su disposición.

El/la trabajador/a queda informado/a de que sus datos personales serán tratados por Ecoembes en el marco de la relación laboral existente entre ambas partes. Dichos datos serán tratados por la organización para las siguientes finalidades:

- Facilitar las gestiones del empleado a la Dirección de Personas y Organización
  - Coordinación de planes de acogida
  - Evaluación continuada del empleado, planes de carrera y formaciones
  - Monitorización de asistencia al puesto de trabajo, gestión de bajas, excedencias, etc.
  - Gestión de beneficios sociales al empleado
  - Gestión de prevención de riesgos laborales
  - Gestión de nóminas
- Agenda de contactos internade los sistemas corporativos de la organización
- Sistema de gestión de incidencias y peticiones de servicio que se registran a través del Servicio CAS, con objeto de su seguimiento y atención.
- Sistema de Gestión de solicitudes de altas, modificaciones y bajas de usuarios del sistema
- Uso de la imagen y/o voz para la difusión en eventos realizados por Ecoembes, en redes sociales, en la web de Ecoembes o en cualquier video o material promocional corporativo de Ecoembes

En el caso de que Ecoembes, considere la realización de algún evento para familiares del trabajador/ trabajadora, los datos necesarios para la organización de los mismos se realizarán previa petición a través de la cumplimentación de un formulario y aceptación del consentimiento para el tratamiento de dichos datos.

Continúa en la página siguiente

Aceptación del Código de Buenas Prácticas en Seguridad de la información y Protección de Datos

En el caso de que el/la trabajador/a consienta expresamente el tratamiento de los datos relativos a su eventual discapacidad para los fines antes señalados, estos únicamente serán comunicados a terceros en cumplimiento de obligaciones legales o con el previo consentimiento de los afectados.

Puedes obtener más información relativa a las finalidades para las que se tratan tus datos, así como de las características adicionales de protección de datos en nuestra **Política de Privacidad de Empleados de Ecoembes.**

Continúa en la página siguiente

Viene de la página anterior

Aceptación del Código de Buenas Prácticas en Seguridad de la información y Protección de Datos

La imagen de los trabajadores será tratada para las finalidades antes señaladas y podrá ser publicada, junto con los datos identificativos, de cargo o puesto ocupado y de contacto profesional, en organigramas o en el directorio Corporativo de la Empresa accesible para todos los trabajadores de la misma a través de la intranet en el marco de la relación laboral para satisfacer intereses legítimos de la Empresa. Los trabajadores pueden oponerse a la publicación de su imagen, siguiendo las indicaciones previstas en el último párrafo de este apartado.

Asimismo, el/la trabajador/a queda informado/a de que, conforme a las leyes vigentes y para las finalidades en ellas previstas, sus datos personales podrán ser comunicados a administraciones o entidades públicas, tales como la autoridad laboral, las autoridades sanitarias, la Seguridad social o la Agencia Tributaria, así como, en su caso, al comité de seguridad y salud de la Empresa, Delegados de prevención, Servicio de Prevención, propio o ajeno, Comité de empresa o Representantes del Personal, de manera no limitativa y que dicho tratamiento se encuentra legitimado por el cumplimiento de obligaciones legales por parte de la Empresa.

Si el/la trabajador/a es beneficiario/a de una póliza de seguro colectiva contratada por la Empresa, este/a consiente que los datos necesarios para la eficacia de la misma, sean comunicados a la entidad aseguradora con la que se contrató, para la tramitación de la correspondiente cobertura y en el supuesto de que se desarrollara un Plan de Compensación Flexible, a las correspondientes empresas que intervengan para ejecutar dicho plan. La Empresa tratará los datos personales de el/la trabajador/a a los que se tenga acceso mientras se mantenga la relación laboral entre las partes. En este sentido, la Empresa conservará los datos personales una vez terminada la relación laboral, debidamente bloqueados, para su puesta a disposición de las Administraciones Públicas competentes, Jueces y Tribunales o el Ministerio Fiscal durante el plazo de prescripción de las acciones que pudieran derivarse de la relación mantenida con el/la trabajador/a y/o los plazos de conservación previstos legalmente.

Rogamos marques la casilla que te corresponda, dándonos tu conformidad:

- ***Pertenezco a Personal de Plantilla***

Con mi firma en este documento muestro mi conformidad y me doy por enterado/a de que el incumplimiento de las normas contenidas en este Código de Buenas Prácticas de Seguridad de la información puede dar lugar a la adopción de las medidas disciplinarias oportunas, pudiendo en algunos casos llegar a ser constitutivo de una infracción laboral muy grave cuya consecuencia puede llevar a la extinción del contrato de trabajo.

- ***Pertenezco a Personal Externo/Subcontratado***

Con mi firma en este documento muestro mi conformidad y me doy por enterado/a de que el incumplimiento de las normas contenidas en este Código de Buenas Prácticas de Seguridad de la información es condición esencial para el correcto desarrollo del contrato vigente con ECOEMBES y que en consecuencia su incumplimiento puede ser causa de resolución del mismo.

Nombre y Apellidos:

Fecha:

Firmar como Personal Externo/Personal de Plantilla

Firma:

ecoembes

CÓDIGO DE BUENAS PRÁCTICAS

EN SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

Julio **2025**

www.ecoembes.com/es