DECÁLOGO DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN

Introducción

El Ayuntamiento de Eibar, en su compromiso para cumplir con el Esquema Nacional de Seguridad, define, documenta y difunde una **Política de Seguridad de la Información** - aprobada mediante Resolución de Alcaldía, de 15 de febrero de 2019- que demuestra el compromiso con la seguridad.

El compromiso se concreta (o se concretará) con el desarrollo próximo de normativas y procedimientos que recogen las obligaciones a las que están sujetas todas las personas usuarias en lo que respecta al tratamiento y seguridad de la información. Entre tanto, con el objeto de garantizar la seguridad, rendimiento y privacidad de los Sistemas Informáticos y de Comunicaciones, los/las usuarios/as deberán de cumplir el presente decálogo.

Dicha información se halla disponible en www.eibar/eus/documentodeseguridad.

1. Usuario/a de los recursos

1.1. Los/as usuarios/as de los Servicios Informáticos o de Comunicación, deberán utilizar con la debida diligencia todos los equipos informáticos, así como toda la infraestructura complementaria. De igual modo, deberán evitar realizar cualquier acción que, de forma voluntaria o no, pueda dañar la integridad física de la instalación (destrozos, sustracción, traslados no autorizados, desensamblado, desconfiguración, etc.).

1.2. Los/as usuarios/as deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento.

1.3. Con la finalidad de detectar y reaccionar ante comportamientos sospechosos o inesperados, se debe establecer o activar sistemas de registro de actividades que almacenen los datos generados por las actividades de sistemas, aplicaciones y usuarios en los activos de información de la Administración General de la CAPV y sus Organismos Autónomos.

2. Uso de cuentas de usuario y credenciales de acceso

2.1. Las cuentas de usuario son personales. En consecuencia, **no se deberá de facilitar el acceso a otras personas**, salvo que se reciba autorización expresa del Responsable de Seguridad y/o del Comité de Seguridad del Ayuntamiento de Eibar.

2.2. Las personas usuarias **son las únicas autorizadas para el uso de la cuenta personal**, y deben ser conscientes de que son responsables de las acciones que se realicen con su identidad sobre los servicios electrónicos sobre los que tengan acceso.

2.3. Las personas usuarias son las **responsables finales de salvaguardar sus claves privadas, y las de cualquier elemento** (tarjeta o dispositivo criptográfico, archivo informático, programa "software", etcétera) **y/o código** (PIN, contraseña, etcétera) que puedan ser necesarios para acceder a las mismas.

2.4. Las personas usuarias deben ser **cuidadosas y diligentes en la custodia y cuidado de las credenciales, la clave privada**, y los **elementos y/o códigos** utilizados para acceder a equipos, servicios y/o información electrónica, **y deben mantenerlas en secreto**, debiendo informar al Departamento de Informática en caso de pérdida o compromiso a la mayor brevedad.

3. Uso de los equipos informáticos

3.1. En ningún caso, se podrán utilizar los recursos informáticos del Ayuntamiento de Eibar para actividades que sean contrarias al ordenamiento jurídico y especialmente, en materia de protección de datos de carácter personal, propiedad intelectual y, en su caso, a las propias del Ayuntamiento de Eibar

3.2. Los equipos informáticos **no deben ser utilizados para fines particulares**.

3.3. Los/as usuarios/as destinarán los medios indicados a usos compatibles con la finalidad de las funciones del servicio al que se encuentren adscritos y que correspondan con su trabajo. Su utilización con cualquier otro fin diferente necesitará del consentimiento expreso de el/la Responsable de Seguridad (Secretario/a general del Ayuntamiento de Eibar).

3.4. **No se podrán modificar los equipos informáticos y periféricos,** así como su conexión a otros equipos ajenos al Ayuntamiento de Eibar, salvo que se obtenga autorización.

3.5. No se extraerá información en soportes digitales o por medios electrónicos, salvo que se cuente con autorización para ello, tomando especiales precauciones en caso de que se trate de información sensible, confidencial o protegida.

3.6. Las tomas de conexión de red del Ayuntamiento de Eibar no pueden ser utilizadas sin el conocimiento y autorización del Departamento de Informática (informatika@eibar.eus). No está permitido conectar dispositivos repetidores ni concentradores, de cable o inalámbricos sin la autorización expresa y previa supervisión por parte de personal técnico del Departamento de Informática.

3.7. Uso de Soportes USB o Magnéticos: Este tipo de dispositivos estará bajo la custodia del usuario que los utilice y deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de terceros no autorizados.

4. Virus informáticos y otro tipo de "malware"

4.1. Todos los equipos de trabajo corporativos (ordenador de sobre mesa, portátil, etc.) deben disponer de mecanismos adecuados para el control de "software" malicioso (virus, gusanos, etcétera), y han de permanecer activados.

4.2. Ante la sospecha de una infección por virus, gusanos, etcétera, se deberá comunicar inmediatamente la incidencia al Departamento de Informática.

5. "Software"

5.1. Para preservar el buen funcionamiento de los servicios electrónicos **se prohíbe la instalación de "software" o programas no corporativos en los equipos de trabajo corporativos**. Si fuera necesaria su instalación, deberá solicitarse al Responsable de Seguridad para que lo analice. Igualmente, no se podrán realizar copias del "software" instalado en los equipos de trabajo.

5.2. Se prohíbe la instalación y utilización de aplicaciones informáticas sin licencia.

5.3. Se prohíbe la descarga o distribución de documentos, libros, imágenes, películas o música infringiendo los derechos de autor y de copia.

5.4. Las personas usuarias no podrán modificar el "software" instalado a nivel corporativo, que en ningún caso deberá ser desactivado.

6. Internet y correo electrónico

6.1. **La utilización del acceso a Internet debe responder a fines profesionales**.

6.2. Por razones de seguridad, se podrán establecer los filtros limitativos que se estimen necesarios para garantizar la seguridad y el buen uso de los accesos a Internet.

6.3. El servicio de correo electrónico del Ayuntamiento de Eibar se utilizará por todas las personas usuarias que se les haya dotado de **cuenta de correo para uso profesional**, debiendo observarse el deber de diligencia en la utilización del mismo.

6.4. Para evitar el correo electrónico masivo no solicitado, también denominado "spam", como regla general, solo se debe dar la dirección de correo electrónico a personas y/o entidades conocidas. No se debe introducir la dirección de correo electrónico en foros o páginas Web no institucionales. Cuando se reciban correos electrónicos desconocidos o no solicitados no se deben contestar, ya que al hacerlo se reconfirma la dirección.

6.5. En el caso de recibir correos electrónicos cuyo remitente y/o contenido sea dudoso, deberá ponerse en contacto inmediatamente con el Departamento de Informática para que se analice.

7. Tratamiento y uso de datos de carácter personal

7.1. Las personas usuarias deben acceder, exclusivamente, a la información necesaria para el desarrollo de las funciones propias de su actividad y únicamente a la que estén autorizadas.

7.2. En el acceso a esta información las personas usuarias están obligadas a cumplir las medidas de seguridad establecidas por la normativa en protección de datos del Ayuntamiento de Eibar (www.eibar.eus/RGPD).

7.3. Todas las personas que intervengan en cualquier fase del tratamiento de datos de carácter personal **están obligadas al secreto profesional respecto de los mismos**.

7.4. Cuando un soporte informático (disco duro, USB, CD...), o documento, en formato electrónico o papel, contenga datos personales, y vaya a ser desechado, se deberán adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada o impresa en los mismos.

7.5. Las personas usuarias que necesiten extraer del Ayuntamiento de Eibar datos de carácter personal deberán solicitar la autorización del Responsable de Seguridad y aplicar las debidas medidas de seguridad para proteger esa información. Asimismo, el Responsable de Seguridad deberá llevar un registro actualizado de la salida de esta información.

7.6. Cualquier incidencia o anomalía que pudiera afectar a la seguridad de los datos personales deberá ser comunicada al Responsable de Seguridad LOPD del Ayuntamiento de Eibar (Director/a de Organización y Personal).

8. Incidentes de seguridad de la información

8.1. Cuando ocurra un incidente que afecte a la seguridad de la información, las personas usuarias deberán reportar el detalle de los hechos acontecidos y de las medidas adoptadas al Responsable de Seguridad, a fin de que se tomen las decisiones oportunas.

9. Mesas limpias y bloqueo del ordenador

9.1. Cuando las personas usuarias se ausenten del puesto de trabajo o dejen desatendido el ordenador **deberán activar el sistema de bloqueo** del que disponga su equipo (salvapantalla protegida por contraseña, bloqueo del terminal, etcétera) con el fin de que se no visualicen datos en la pantalla, así como evitar que se acceda al equipo o aplicaciones por terceros no autorizados.

9.2. Del mismo modo todos los documentos en papel que contengan datos de carácter personal deberán ser custodiados en todo momento, mientras estén siendo usados, por la persona a cargo, evitando el acceso por personas no autorizadas.

10. Monitorización de la actividad

10.1. El Ayuntamiento de Eibar, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente podrá:

- Revisar el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizar los accesos a la información contenida en sus sistemas.
- Auditar la seguridad de las credenciales y aplicaciones.
- Monitorizar los servicios de internet, correo electrónico y otras herramientas de colaboración.

10.2. El Ayuntamiento de Eibar llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios\as.