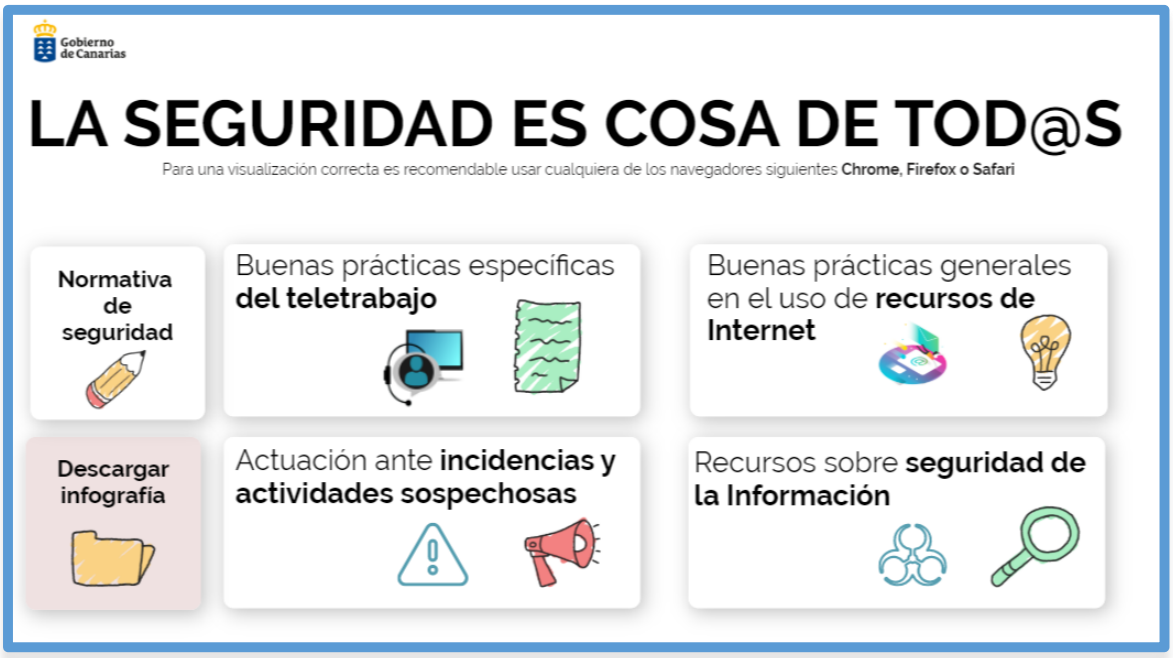
GUÍA "MEDIDAS DE SEGURIDAD"

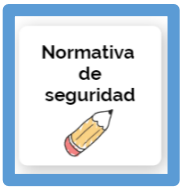
Contenido

Accede a la infografía:



Introducción

Las Instrucciones que conforman la normativa de seguridad en el uso de los recursos informáticos, telefónicos y de redes de comunicación de la Administración Pública de la Comunidad Autónoma de Canarias, aprobada mediante Acuerdo de Gobierno publicado por Resolución de Presidencia de Gobierno, de 25 de junio de 2018, detallan las normas consensuadas en el Gobierno de Canarias que deben seguirse para hacer un uso seguro de los recursos corporativos, en cumplimiento del Esquema Nacional de Seguridad.



A fin de afrontar la actual situación de Estado de Alarma como consecuencia del COVID-19, a nivel estatal y autonómico se ha promovido la realización de la actividad laboral de forma remota, generalizando así el uso del teletrabajo y permitiendo la salida de documentación corporativa de los respectivos centros de trabajo. Este tipo de actividad profesional implica una responsabilidad sobre la utilización de los medios de teletrabajo y la custodia de la documentación corporativa.

Estas circunstancias hacen conveniente concretar, en línea con las mencionadas Instrucciones, una serie de buenas prácticas que en conjunto permitan contribuir a garantizar la seguridad de los sistemas de información, manteniendo segura la información del Gobierno de Canarias.

Un ordenador seguro, una red segura, y un usuario concienciado forman el mejor equipo para evitar riesgos derivados del trabajo desde sistemas no presenciales.

Buenas prácticas específicas del teletrabajo

- ## Equipo de acceso a la red del Gobierno de Canarias

Si usas **un equipo personal** para conectarte por VPN a la red corporativa del Gobierno de Canarias:

- Asegura que el equipo tiene instalado **un antivirus** y que este está habilitado en todo momento, a fin de que pueda detectar cualquier posible malware que te llegue.
- Reinicia el equipo regularmente para que se apliquen las **actualizaciones oficiales** que vayan publicando los distintos fabricantes, a fin de tener siempre actualizado el sistema operativo, las aplicaciones que tengas instaladas, entre ellas el navegador web, y el antivirus.
- En la medida de lo posible, y especialmente si el equipo es compartido entre varias personas, utiliza una **cuenta específica para tu uso exclusivo en el equipo.**

En caso de utilizar **equipos corporativos**:

- Extrema las medidas de seguridad para la custodia del equipo asignado.

Sea cual sea el equipo que utilices:

- Evita la instalación de cualquier **software o contenido dudoso**, y la conexión de dispositivos USB para los que no tengas plena confianza en que estén libres de virus.
- No copies **información corporativa** al equipo. Esta debe siempre almacenarse de forma centralizada en los sistemas del Gobierno de Canarias.

Conexión a la red del Gobierno de Canarias

- **No utilices conexiones WIFI abiertas ni redes públicas**. En caso de tener que conectarte desde un lugar público, es recomendable utilizar un módem USB con conexión 4G/5G, mucho más seguros que cualquier red pública ajena.

- Si te conectas desde tu domicilio, es conveniente que actualices la clave de la WIFI frecuentemente, con una contraseña robusta, larga y que contenga caracteres alfanuméricos.

- En el acceso a las aplicaciones y sistemas de información corporativo utiliza, siempre que sea posible, el acceso con certificado digital.

- **Al acabar la jornada de teletrabajo:**

    - Cierra todas las conexiones a los sistemas de información y webs corporativas.
    - Desconecta la conexión VPN tal como se describe en el correspondiente manual de conexión remota al equipo del puesto de trabajo.

- ## Reuniones y videoconferencias

No hagas uso de programas o servicios de Internet **no corporativos** (Zoom, Skype, etc.) para las reuniones laborales que tengan contenido sensible o confidencial. El uso de este tipo de aplicaciones debe limitarse a casos específicos en los que no haya contenido sensible.

RECUERDA QUE PARA LAS REUNIONES LABORALES TIENES A TU DISPOSICIÓN HERRAMIENTAS CORPORATIVAS DE VIDECONFERENCIA

- ## Confidencialidad de la información y protección de datos personales

- Sé respetuoso con **el deber de secreto profesional** al que estamos obligados, y evita el acceso a información corporativa por familiares o terceros.

- **No apuntes las contraseñas corporativas** en ningún lugar.

- Solo se deben sacar documentos fuera de las oficinas cuando resulte estrictamente necesario y siempre debe ser **un movimiento autorizado por el responsable correspondiente.**

- Extrema las medidas de seguridad para la custodia de **documentación en papel y dispositivos de almacenamiento portables** (memorias USB, discos duros extraíbles, DVDs, etc.) que manejes en el entorno no laboral, guardándolos en un armario o cajón, a poder ser bajo llave.

- Si debes deshacerte de algún documento, rómpelo antes de depositarlo en papeleras o contenedores de reciclaje. Esto es especialmente importante si contiene información sensible o datos sobre personas físicas.

- No copies información corporativa a **servicios de terceros en la nub**e (Google, Gmail, Dropbox…). Si necesitas compartir ficheros grandes, puedes hacer uso de la solución corporativa GobBox.

- Los sistemas corporativos garantizan la confidencialidad de los datos, siendo responsable de su protección el órgano u organismo que sea responsable de la correspondiente actividad de tratamiento, conforme a la legislación vigente en materia de protección de datos. Puedes consultar las actividades de tratamiento actualmente registradas en este enlace.

VER TAMBIÉN INFOGRAFÍAS SOBRE

Orientaciones básicas sobre protección de datos personales	8 Consejos básicos sobre seguridad
	

Buenas prácticas generales en el uso de recursos de Internet

- ## Navegación segura por internet y la web

- Evita navegar por páginas **web no seguras y de dudosa reputación**.

- Cuando te conectes vía web **verifica en la barra del navegador que la dirección web del destino es la correcta**. Los ciberdelincuentes pueden replicar completamente una web y robarte tu contraseña.

- **No hagas uso de la funcionalidad de recordar contraseña** que ofrecen los navegadores web (Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer, Safari, etc.).

- **Elimina periódicamente el historial de navegación**, cookies, contraseñas recordadas y otros archivos temporales. Así evitamos potenciales elementos espías.

- **No utilices tu cuenta corporativa en servicios de Internet personales o ajenos al Gobierno de Canarias**, ni utilices en estos servicios la misma contraseña que tienes en tu cuenta corporativa. De hacerlo así, corres el riesgo de que te roben tus credenciales y accedan con ellas a la información de tu cuenta corporativa en el Gobierno de Canarias.

• Uso seguro del correo electrónico

- **No emplees cuentas de correo ajenas al Gobierno de Canarias para tratar asuntos laborales,** ni reenvíes correos laborales a cuentas de correo personales ajenas al Gobierno de Canarias.

- Al incluir a nuevos destinatarios en mensajes que vayas a responder o reenviar, **revisa la información contenida** en el hilo de correos para confirmar que es apta para esos nuevos remitentes.

- **Cifra los mensajes de correo** que contengan información clasificada o sensible.

- Extrema la precaución ante correos recibidos que puedan ser sospechosos para evitar ser víctima de ciberdelitos habituales como el phishing, consistente en la recepción de una comunicación aparentemente legítima que, a través de una acción que solicita (actualizar, confirmar información mediante un enlace, abrir un documento adjunto, etc.) busca robar información o desplegar malware. **Las principales medidas de prevención a considerar son:**
    - No confíes únicamente en el nombre del remitente; **verifica si el dominio del correo recibido** (la parte que sigue a '@') es de confianza, por ejemplo **'gobiernodecanarias.org', 'justiciaencanarias.org' o 'canarias.org'**. Incluso si verificas que se trata de un contacto legítimo pero el contenido del correo te genera desconfianza, contacta con el mismo por otra vía de comunicación para verificar la legitimidad, ya que su cuenta puede haber sido robada.
    - Sospecha de correos electrónicos que presenten cualquier **patrón fuera de lo habitua**l, como solicitar información inusual (contraseña, datos personales, etc.) o realizar actuaciones sospechosas (renovar contraseña a través de un enlace, descarga o ejecución de un adjunto, etc.).
    - **No hagas clic en enlaces de correos sospechosos**; verifica su ortografía y tecléala de forma manual en la barra del navegador.
    - **No abras ningún archivo adjunto de correos electrónicos sospechosos**, ni te fíes del icono asociado al fichero. En caso de correos aparentemente legítimos de los que desconfías de su contenido, antes de abrirlo asegúrate de que la extensión del archivo adjunto (la parte que sigue al '.') no es sospechosa (no abras nunca

ficheros .vbs o .exe) y analízalo con el antivirus que tengas instalado en tu equipo.

- **No habilites las macros de los documentos ofimáticos** (Word, Excel, PowerPoint, LibreOffice, …), incluso si el propio fichero así lo solicita, y no habilites el modo edición para no desactivar la protección que ofrece la propia herramienta ofimática.
- No respondas a comunicaciones sospechosas ni realices ninguna acción que proporcione datos personales o de tu cuenta de acceso.

• Actuación ante incidencias y actividades sospechosas

- Ante cualquier sospecha de que tu cuenta corporativa puede haber sido comprometida, puedes actuar de primera mano para bloquear el presunto incidente cambiando lo antes posible tu contraseña a través de MiClave.

- En cualquier caso, recuerda que debes notificar a CiberCentro con carácter inmediato cualquier situación que pueda comprometer la seguridad de la información o de los sistemas del Gobierno de Canarias (si recibes un correo o llamada sospechosa, o detectas un uso inusual de tu cuenta corporativa, o cualquier otro evento anómalo), para su adecuada gestión.

- Puedes realizar esta comunicación a través de cualquiera de los canales habilitados: Sírvete, teléfono (912 desde dentro de la red corporativa, o 922 922 912 - 928 117 912 desde fuera) o correo electrónico (cibercentro@gobiernodecanarias.org).

- Cuando abras una incidencia en CiberCentro recuerda adjuntar cualquier evidencia que tengas, como el correo sospechoso recibido para agilizar la gestión.

Acceda al formulario de contacto
O llame a:
Teléfono interno 912
Teléfonos: 922 922 912- 928 117 912

- **Recursos sobre Seguridad de la Información**

La Dirección General de Telecomunicaciones y Nuevas Tecnologías pone a tu disposición una serie de recursos como son las **FAQs sobre incidentes de seguridad** y los **boletines que se publican periódicamente**, así como las distintas **Normativas que están aprobadas**, todo ello accesible a través de los siguientes enlaces de la página web de CiberCentro

SEGURIDAD	NORMATIVA	BOLETINES **Acceso a los boletines**
	 Sólo visible desde la intranet	 **Mantente informado (Suscripción)**