

# HAZ

**buen uso de la información a la que tienes acceso.**

Prevé y evita cualquier operación que pueda producir una alteración indebida inutilización, destrucción, robo, revelación o uso no autorizado de la misma.

# USA

**de manera responsable los equipos proporcionados** y sólo para el desarrollo de tus funciones profesionales.

# EVITA

**almacenar información en dispositivos de almacenamiento extraíble** (discos duros portátiles, memorias USB, etc).

# GUARDA

**tus contraseñas en un sitio seguro** y si crees que alguien ha podido conocerlas, avisa cuanto antes.

# NO DEJES

**los documentos a la vista, tu equipo a otras personas.**

# PROTEGE

**tu ordenador evitando visitar páginas no fiables o sospechosas** para evitar posibles incidentes de seguridad, en especial, las que se consideren susceptibles de contener código dañino o malicioso.



# HAZ

**buen uso de tu cuenta de correo electrónico corporativo.** Revísalo con frecuencia para evitar demoras en el desempeño de tus funciones y habilita la respuesta automática en caso de ausencia por un período determinado.

# USA

**las herramientas corporativas** para el intercambio de ficheros que superen el límite establecido en el sistema de correo electrónico.

# EVITA

**que la información en formato papel** quede sobre la mesas de trabajo al final de la jornada.

# GUARDA

**la información que precises** para el desempeño de tus funciones en los sistemas de información, en las herramientas corporativas o en las estructuras comunes de almacenamiento habilitados por la Administración.

# NO DEJES

**tu contraseña guardada en un dispositivo** que no vayas a utilizar, en especial, en situaciones de renovación de equipo, renovación de teléfono móvil, traslado o uso temporal o provisional de un equipo.

# PROTEGE

**tu sesión cuando termines de usar cualquier aplicación.** Ciérrala correctamente utilizando las funcionalidades 'desconexión', 'cerrar sesión' o 'salir'.

