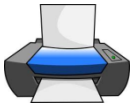
GUÍA DE BUENAS PRÁCTICAS
EN SEGURIDAD DE LA INFORMACIÓN

	Normativa de obligado cumplimiento	
¿Qué es un dato personal?	Tu usuario es personal, te identifica y autentifica. No debes compartirlo con nadie. Debes guardarlo con el mismo celo con el que guardas las llaves de casa, es la puerta de acceso a tu trabajo.	
Evita las contraseñas fáciles de adivinar	Evita contraseñas de acceso fácilmente adivinables: fecha de cumpleaños, número de DNI, mes del año en curso, etc. Utiliza contraseñas fáciles de recordar para ti y difíciles de adivinar por otras personas. Memoriza tus contraseñas y bajo ningún concepto, la apuntes en cuadernos, hojas de notas, junto al PC.	
Bloquea el ordenador siempre que abandones tu puesto de trabajo	Cuando abandones tu puesto de trabajo, deja el PC bloqueado y asegúrate que es necesario volver a introducir la contraseña para poder acceder nuevamente. Al final del día, deja tu equipo completamente apagado.	
No envíes ninguna contraseña por correo electrónico	Nunca envíes por correo electrónico datos de tu usuario y/o contraseña.	
Notifica cualquier incidencia de Seguridad	**Recuerda que debes de notificar cualquier incidencia de seguridad de la información. Es una obligación legal.** **https://hcs.es/intranet/download_file.cfm?file=22035&area=2026&open=1** **Si detectas que accedes a información que no es necesaria para tus funciones dentro de la empresa, comunícalo inmediatamente al departamento de Informática o a tu responsable más inmediato.** **Toda incidencia que pueda comprometer la seguridad de la información debe ser reportada lo antes posibles.**	
Deja siempre tu mesa limpia	Toda la documentación en papel debes guardarla en armarios cerrados, preferiblemente bajo llave, sin que queden a la vista de personas no autorizadas. Al finalizar tu jornada laboral, recuerda que los documentos han de quedar fuera del alcance de personas ajenas.	
Destruye el papel	Siempre que haya que destruir un papel que contenga información confidencial, incluyendo cualquier tipo de datos personales, utiliza las destructoras de papel. Si no tuvieras una cerca, trocea al máximo el papel y tíralos en varias papeleras.	
Evita imprimir datos	Evita, en la medida de lo posible, imprimir documentos o datos almacenados en los Sistemas Informáticos de la empresa. En caso de que sea necesario imprimirlos, destrúyelos en el momento que dejen de ser útiles.	
No saques información de las instalaciones	Queda terminantemente prohibido sacar información (física o electrónica), sobre todo si ésta contiene información con datos de carácter personal, sin autorización. La salida de información debe estar expresamente autorizada.	
Uso del Antivirus	Mantén activado el antivirus para proteger el equipo y su contenido ante cualquier amenazada. Sobre todo cuando se navega por internet usa tu sentido común y consulta en caso de duda.	

GUÍA DE BUENAS PRÁCTICAS
EN SEGURIDAD DE LA INFORMACIÓN

	Normativa de obligado cumplimiento	
Uso de medios removibles	No dejes el portátil desatendido en lugares públicos. Utiliza un candado físico si tienes que ausentarte o lleva el equipo contigo. Elimina datos innecesarios del portátil y/o cifra el contenido del portátil para evitar el acceso a los datos en caso de robo del equipo.	
Uso de dispositivos móviles (notebooks, tablets, smartphones, etc.) durante la Navegación	Asegúrate sobre la confianza o acreditación de los sitios web antes de proceder a descargar archivos. Evita la descarga e instalación de ficheros procedentes de fuentes desconocidas. Verifica la procedencia y fiabilidad de los ficheros adjuntos en su correo electrónico. Realiza transacciones bancarias desde ordenadores seguros. Borra las cookies, los ficheros temporales y el historial cuando utilices equipos ajenos (públicos o de otras personas) para no dejar rastro de tu navegación.	
Uso del Correo Electrónico	Usa el correo electrónico a los fines corporativos. Recuerda que un uso inadecuado del correo electrónico puede llegar a consumir una parte excesiva de los recursos disponibles (tanto nuestros como de los servidores corporativos que nos prestan el servicio), causándonos problemas a nosotros mismos y al resto de empleados de la organización.	
Copias de Seguridad	Guarda siempre los datos en los servidores, puesto que al realizarse copias periódicas de seguridad, aseguran la recuperación de los datos ante cualquier incidencia.	
Autorizaciones	Debes solicitar autorización expresa para realizar determinadas operaciones como: ▪ Ceder datos de carácter personal a otras empresas/personas. ▪ Acceder desde el exterior de las instalaciones. ▪ Sacar soportes, equipos portátiles o documentos que contengan datos de carácter personal (inclusive enviados por correo electrónico).	
Registro de Soportes/ Documentos	Asegúrate de que los soportes y documentos con datos personales sólo son accesibles por el personal autorizado, deben permitir identificar el tipo de información que contienen a estas personas y ser inventariados.	
Registro de entrada y Salida	Controla la salida y entrada de soportes a través del registro, de modo que se pueda conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.	
Cifrado de los datos	Si manejas datos de **CATEGORIAS ESPECIALES** asegúrate que los mismos son cifrados cuando estos se encuentren en dispositivos portátiles y están fuera de las instalaciones.