| **CUESTIONARIO SOBRE MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN**  **Apellidos y Nombre:**  **Departamento: ESTOMATOLOGÍA** | | |
| --- | --- | --- |
| **1.-** | **Marco Operacional Control de acceso** | **SI= 1**  **No=0**  **No procede= 2** |
| **ejemplo** | **No deja ordenadores sin proteger** | 1 |
| **1.1** | **No deja ordenadores sin proteger** |  |
| **1.2** | **No deja claves escritas en post-it pegados** |  |
| **1.3** | **El nombre de usuario identifica a una sola persona.** |  |
| **1.4** | **Usuarios diferentes para roles diferentes** |  |
| **1.5** | **Periodo de retención de cuentas** |  |
| **1.6** | **Asignación de privilegios imprescindibles.** |  |
| **1.7** | **Credenciales de accesos bajo el exclusivo control del usuario.** |  |
| **1.8** | **Limitación del número de intentos de acceso.** |  |
| **1.9** | **Registro de intentos de acceso.** |  |
| **1.10** | **Autocontrol de acceso del usuario** |  |
| **1.11** | **Uso de VPN para acceso remoto.** |  |
| **2.-** | **Marco Operacional Explotación: medidas** | **SI= 1**  **No=0**  **No procede= 2** |
| **2.1** | **Inventario de ordenadores.** |  |
| **2.2** | **Elimina las cuentas de usuario que trae por defecto el equipo.** |  |
| **2.3** | **Cambia la clave que trae el ordenador instalada por defecto.** |  |
| **2.4** | **Cambio de claves/password.** |  |
| **2.5** | **Mantiene los sistemas actualizados.** |  |
| **2.6** | **Comunica incidente de seguridad, o sospecha.** |  |
| **2.7** | **Antivirus actualizado.** |  |
| **2.8** | **Mecanismo de detección de intrusión en el equipo.** |  |
|  |  |  |
| **3.-** | **Medidas de protección: Instalaciones** | **SI= 1**  **No=0**  **No procede= 2** |
| **3.1** | **Equipos fácilmente accesibles físicamente, en una caja cerrada con llave y ventilada.** |  |
| **3.2** | **Protección de corriente en servidores.** |  |
| **3.3** | **Acceso físico al ordenador controlado.** |  |
| **3.4** | **Control de entrada y salida de dispositivos.** |  |
| **4.-** | **Medidas de protección:  Protección de equipos** | **SI= 1**  **No=0**  **No procede= 2** |
| **4.1** | **Puesto de trabajo despejados.** |  |
| **4.2** | **El ordenador se bloquea al cabo de un tiempo de inactividad de forma automática.** |  |
| **4.3** | **Cuando abandona el ordenador lo deja bloqueado.** |  |
| **5.-** | **Medidas de protección: Protección de los soportes de información** | **SI= 1**  **No=0**  **No procede= 2** |
| **5.1** | **Etiqueta de soportes de la información con indicación del nivel de seguridad asignado.** |  |
| **5.2** | **Se cifran los dispositivos removibles tales como DVD, CD, discos USB y otros similares.** |  |
| **5.3** | **Se aplican medidas de acceso a los soportes de información.** |  |
| **5.4** | **Los dispositivos permanecen bajo control, en los desplazamientos.** |  |
| **5.5** | **Cuando deja de utilizar los soportes se borran y/o destruyen de forma segura.** |  |
| **5.6** | **En el caso de reutilización de cintas para copias de seguridad se borra previamente a grabar algo en ellas.** |  |
| **5.7** | **Realiza copias de seguridad que permitan recuperar los datos perdidos.** |  |
| **5.8** | **Cuando envía documentos retira toda la información adicional contenida en campos ocultos** |  |
| **5.9** | **Retira la información obsoleta publicada en las páginas web.** |  |
| **5.10** | **Hay establecido un sistema de control de acceso a impresoras compartidas.** |  |
| **5.11** | **Solo hace copias de documentos cuando resulta estrictamente necesario.** |  |
| **6.-** | **Medidas de protección de datos en Papel** | **SI= 1**  **No=0**  **No procede= 2** |
| **6.1** | **Practica política de mesas limpias** |  |
| **6.2** | **Destructora de pape**l (Destrucción de documentos). |  |
| **6.3** | **Datos bajo llave, acceso a la información controlada** (Custodia información). |  |
| **6.4** | **Registro de control de acceso a datos sensibles; Datos de características especiales.** |  |
| **6.5** | **Traslado físico.** |  |
| **6.6** | **Etiquetado de carpetas.** |  |
| **6.7** | **Criterios de archivo para la correcta conservación de documentos.** |  |
| **7.-** | **Medidas de protección para almacenamiento de datos personales en la NUBE y APPs (éstas en la medida de lo posible)** | **SI= 1**  **No=0**  **No procede= 2** |
| **7.1** | **Claves seguras y diferentes para cada uno de los servicios de la nube.** |  |
| **7.2** | **Cifrado de información sensible.** |  |
| **7.3** | **Copias de Seguridad.** |  |
| **7.4** | **Segundo factor de autenticación (2FA).** |  |
| **7.5** | **Trasferencia securizada.** |  |
| **7.6** | **Exponer datos lo menos posible**. |  |
| **7.7** | **Criterios de archivo.** |  |
| **7.8** | **Utilizar servicios propios de UGR.** |  |
| **7.9** | **Localización de los datos en el caso de nubes públicas.** |  |
| **7.10** | **Tener contrato con el proveedor de la nube pública.** |  |
| **7.11** | **Compartición de ficheros con datos personales con clave de recurso compartido.** |  |
|  |  |  |
| **8.- OBSERVACIONES** | | |