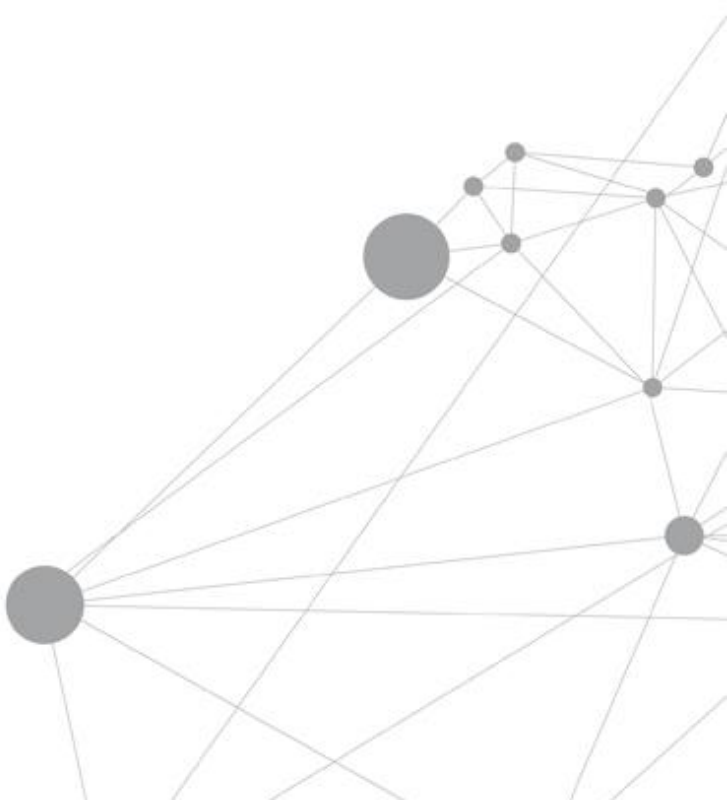
POLÍTICAS DE CIBERSEGURIDAD

EMPLEADOS

Dpto. TIC Grupo Diseños NT

05/10/2022



1. PROTECCIÓN DEL PUESTO DE TRABAJO

1.1 Objetivos

Garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de trabajo.

1.2 Puntos clave

- **Uso de medios de almacenamiento.** Para guardar o compartir información, tanto con compañeros o nosotros mismos, como con agentes externos, debemos usar las herramientas que nos proporciona nuestra licencia de Microsoft. Estas son *One Drive* y *Share Point*.
- **Uso de medios de almacenamiento extraíbles.** En el caso de que sea necesario el uso de dispositivos de almacenamiento portables; como discos duros, pendrives o tarjetas de memoria; el equipo situado en la sala "La Pecera" tendrá habilitado un lector de dispositivos para hacer uso de estos medios. Existe una solución en el portal FreshDesk que describe el procedimiento a llevar a cabo en este caso.
- **Política de mesas limpias.** Conocemos como política de mesas limpias la obligación de guardar la documentación de trabajo al ausentarse del puesto y al terminar la jornada laboral. No se debe dejar información sensible a la vista de personas que pudieran hacer un uso indebido de la misma. Todo ello conlleva:
  - Mantener el puesto de trabajo limpio y ordenado;
  - Guardar la documentación y dispositivos extraíbles que no se están siendo usados en ese momento, especialmente al ausentarnos del puesto y al fin de la jornada laboral;
  - No apuntar usuario ni contraseñas en *post-it* o similares.
- **Destrucción básica de documentación mediante mecanismos seguros.** Todo el personal debe utilizar destructoras de papel para eliminar la información confidencial.
- **No abandonar documentación sensible en impresoras o escáneres.** Para evitar que la información acabe en manos no deseadas el usuario debe:
  - Recoger inmediatamente aquellos documentos enviados a imprimir;
  - Guardar la documentación una vez escaneada;
  - Utilizar los mecanismos de impresión segura.
- **No revelar información a usuarios no debidamente identificados.** La información es uno de los activos empresariales más importantes. Por ello es posible que alguien intente obtener parte de esta información (contraseñas, información financiera, etc.) engañando a un empleado. Esta práctica se conoce como ingeniería social.
  Los delincuentes se hacen pasar por algún responsable, persona o empresa conocida para que el empleado se confíe y facilite la información que le

solicitan empleando para ello una llamada telefónica, el correo electrónico, las redes sociales o mensajes del tipo SMS o Whatsapp.

- **Obligación de confidencialidad.** El empleado debe aceptar un compromiso de confidencialidad relativo a cualquier información a la que tenga acceso durante su participación laboral en la empresa. La obligación de confidencialidad tendrá validez todo el tiempo que se haya exigido en el contrato laboral. La información debe protegerse aun cuando el empleado ya no forma parte de la empresa.
- **Uso de las contraseñas.** El usuario debe seguir la Política de contraseñas:
    - las credenciales (usuario y contraseña) son confidenciales y no pueden ser publicadas ni compartidas;
    - no deben anotarse las credenciales en documentos ni en cualquier otro tipo de soporte;
    - las contraseñas deben ser robustas: mínimo 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,], ?, etc.);
    - se deben cambiar cada 120 días, sin repetir ni secuenciar contraseñas anteriores y no utilizar en páginas web, comercios electrónicos o aplicaciones personales.
- **Obligación de bloqueo de sesión y apagado de equipo.** Para evitar el acceso indebido o por personal no autorizado al equipo del puesto de trabajo:
    - el empleado deberá bloquearlo cada vez que se ausente de su puesto;
    - el empleado apagará su equipo al finalizar la jornada laboral.
- **Uso adecuado de Internet.** El empleado debe conocer, aceptar y aplicar la normativa que regula el uso de Internet como herramienta de trabajo con los usos permitidos y prohibidos. También seguirá las recomendaciones de seguridad relativas a la navegación por internet como:
    - verificar que las direcciones (URL) de destino son correctas;
    - verificar que el certificado es válido, cuando se trate de conexiones a entrornos seguros (webmail, extranet, etc.) o realicemos transacciones;
    - comprobar que se cumple el protocolo *https://* en las páginas donde trabajemos con información crítica.
- **Uso de portátiles y dispositivos móviles propiedad de la empresa.** El empleado debe conocer, aceptar (con su firma) y aplicar la Política de uso de dispositivos móviles de la empresa.
- **Cifrado de la información confidencial.** El empleado debe conocer, aceptar (con su firma) y aplicar la Política de uso de tecnologías criptográficas y la Política de clasificación de información que indica que información debe ser cifrada.
- **Obligación de notificar incidentes de seguridad.** El empleado debe advertir de cualquier incidente relacionado con su puesto de trabajo:
    - alertas de virus/malware generadas por el antivirus;
    - llamadas sospechosas recibidas pidiendo información sensible;
    - correos electrónicos que contengan virus;
    - pérdida de dispositivos móviles (portátiles, *smartphones*, o *tablets*) y dispositivos de almacenamiento externos (USB, discos duros, etc);

- borrado accidental de la información;
- alteración accidental de datos o registros en las aplicaciones con información crítica;
- comportamientos anómalos de los sistemas de información;
- hallazgo de información en ubicaciones no designadas para ello;
- evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (CPD, despachos, almacenes…);
- evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros;
- cualquier actividad sospechosa que pueda detectar en su puesto de trabajo.

2. USO DE WIFI Y REDES EXTERNAS

2.1 Objetivos

Garantizar la seguridad de los datos y comunicaciones corporativos cuando el acceso a los mismos tiene lugar desde fuera de las instalaciones de la empresa mediante la utilización de redes externas no corporativas.

2.2 Puntos clave

- **Política de conexión.** El acceso, tanto a la red como a las aplicaciones corporativas, queda restringido a los dispositivos proporcionados por el departamento TIC del grupo. En determinados casos, bajo estricta autorización y supervisión de dicho departamento, se otorgarán permisos para el uso de estas herramientas al trabajador que lo necesite, previa petición por su responsable de departamento.
- **Configuración de la VPN.** Para los accesos permitidos desde el exterior se dispone de un servicio VPN. Para el uso de este servicio se debe generar una petición en el portal de soporte *FreshDesk*.
- **Uso de la VPN.** Los empleados que lo tengan autorizado el acceso vía VPN conocerán cómo hacerlo y cuándo está permitido:
  - cuando utilicemos cualquier red pública fuera de la red corporativa;
  - para acceder a los recursos corporativos como impresoras, documentos, aplicaciones específicas, etc.;
  - cuando necesitemos realizar operaciones confidenciales: banca online, facturación, transmisión de credenciales, etc.;
  - cuando hagamos uso del teletrabajo.
- **Redes inalámbricas de los dispositivos móviles.** Activar la conexión wifi, *bluetooth* o antena GPS únicamente en los momentos que se vayan a utilizar y con las convenientes medidas de seguridad.
- **Uso de dispositivos móviles.** Si utilizas dispositivos móviles para trabajar fuera de la empresa, se han de tomar las medidas de seguridad indicadas en las

Políticas de uso de dispositivos móviles corporativos y en la de uso de dispositivos móviles no corporativos.

- **Uso de ordenadores no corporativos.** Si utilizas ordenadores de uso público evita realizar actividades de alto riesgo (uso de email o cualquier aplicación corporativa, trabajar con documentos online, redes sociales, banca online, etc..). Desconfía de la seguridad del equipo y sus conexiones. En cualquier caso, si te vieras en la necesidad de utilizarlos para hacer *login* en algún servicio corporativos siempre que esté permitido y no puedas hacer uso de una VPN:
    - revisa el entorno para evitar la mirada de observadores o de cámaras;
    - utiliza el modo de navegación privada del navegador;
    - teclea la URL o la dirección web, en lugar de utilizar el buscador;
    - verifica que la página a la que accedes es auténtica, que utiliza protocolo *https://* y que tiene certificado y está vigente.
    - evita que el navegador guarde las contraseñas.
    - al finalizar la sesión borra el historial de navegación y las cookies en el navegador;
    - revisas que no dejas ningún archivo personal en el equipo;
    - actualiza el software de sistemas operativos y aplicaciones;
    - utiliza un usuario no compartido;
    - instala y activa un antivirus y el cortafuegos del sistema operativo;
    - no instales aplicaciones sin licencia o cuyo origen desconozcas.

3. USO DEL CORREO ELECTRÓNICO

3.1 Objetivos

Establecer unas normas de uso permitido y seguro del correo electrónico corporativo que sirva para impedir errores, incidentes y usos ilícitos, y para evitar ataques por esta vía.

3.2 Puntos clave

- **Contraseña segura.** Todas las cuentas deben utilizar contraseñas de acceso de acuerdo con la Política de contraseñas, se recomienda:
    - usar una contraseña segura para evitar accesos no autorizados;
    - utilizar el doble factor de autenticación;
    - si se accede a través de una interfaz web, nunca recordad la contraseña.
- **Correos sospechosos.** Los empleados deben aprender a identificar correos fraudulentos y sospechar cuando:
    - el cuerpo del mensaje presente cambios de aspecto (logotipos, pie de firma, etc.) con respecto a los mensajes recibidos anteriormente por ese mismo remitente;
    - el mensaje contiene una “llamada a la acción” que nos urge, invita, o solicita llevar a cabo algo no habitual;

- se soliciten credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.).

- **Identificación de remitente.** El empleado no abrirá un correo sin identificar el remitente. Si el remitente no es un contacto conocido habrá que prestar especial atención ya que puede tratarse de un nuevo cliente o de un correo malicioso.
  Si el remitente es un contacto conocido, pero por otros motivos (cuerpo del mensaje, archivos adjuntos, enlaces, etc.) sospechas que se ha podido suplantar su identidad, debes contactar con éste por otro medio para confirmar su identidad.
- **Análisis de adjuntos.** Al recibir un mensaje con un adjunto, este se debe analizar cuidadosamente antes de abrirlo. Aunque el remitente sea conocido puede haber sido suplantado y no apercibirnos. La descarga de adjuntos maliciosos podría infectar nuestros equipos con algún tipo de malware. Tener el antivirus activo y actualizado puede ayudarnos a identificar los archivos maliciosos. Estas son algunas medidas para identificar un adjunto malicioso:
  - tiene un nombre que nos incita a descargarlo, por ser habitual o porque creemos que tiene un contenido atractivo;
  - el icono no corresponde con el tipo de archivo (su extensión), se suelen ocultar ficheros ejecutables bajo iconos de aplicaciones como Word, PDF, Excel, etc.;
  - tiene una extensión familiar, pero en realidad está seguida de muchos espacios para que no veamos la extensión real (ejecutable) en nuestro explorador de ficheros, por ejemplo: listadoanual.pdf .exe;
  - nos pide habilitar opciones deshabilitadas por defecto como el uso de macros;
  - no reconoces la extensión del adjunto y puede que se trate de un archivo ejecutable (hay muchas extensiones con las que no estamos familiarizados);
  - es o encubre un archivo JavaScript (archivos con extensión .js).
- **Inspección de enlaces.** Al recibir un mensaje con un enlace, antes de hacer clic el receptor debe:
  - revisar la URL, sitúate sobre el texto del enlace, para visualizar la dirección antes de hacer clic en él;
  - identificar enlaces sospechosos que se parecen a enlaces legítimos fijándonos en que:
    - pueden tener letras o caracteres de más o de menos y pasarnos desapercibidas;
    - podrían estar utilizando homógrafos, es decir caracteres que se parecen entres sí en determinadas tipografías (1 y l, O y 0).
- **No responder al spam (correo basura).** Cuando recibimos correo no deseado no respondemos al mismo. De lo contrario confirmaremos que la cuenta está activa y seremos foco de futuros ataques. Agrégalo a tu lista de spam y elimínalo. Tampoco lo reenviaremos en caso de cadenas de mensajes.
- **Utilizar la copia oculta (BCC o CCO).** Cuando se envíen mensajes a múltiples destinatarios, envíatelo a ti mismo y utiliza la opción de copia oculta, (CCO o BCO en la mayoría de los clientes de correo) en lugar de la copia normal CC. La

copia oculta impide que los destinatarios vean a quién más ha sido enviado. De esta forma evitaremos que cualquiera pueda hacerse con unas cuantas direcciones de correo válidas a las que enviar spam o mensajes fraudulentos. Recuerda que el correo electrónico es un dato personal de nuestros clientes y usuarios, que no debemos utilizar para otros fines distintos de aquellos para los que fue solicitado. No debemos divulgarlo o comunicarlo a terceros sin su consentimiento.

- **Reenvío de correos.** Se informará de la prohibición del reenvío de correos corporativos a cuentas personales salvo casos excepcionales que deben ser autorizados por la dirección.
- **Evitar las redes públicas.** Evitar utilizar el correo electrónico desde conexiones públicas (la wifi de una cafetería, el ordenador de un hotel, etc.) de acuerdo con la Política de uso de wifis y conexiones externas ya que nuestro tráfico de datos puede ser interceptado por cualquier usuario de esta red. Como alternativa, es preferible utilizar redes de telefonía móvil como el 3G o 4G.
- **Uso apropiado del correo corporativo.** El empleado conoce y acepta la normativa relativa al uso del correo corporativo.

4. USO DE DISPOSITIVOS MÓVILES NO CORPORATIVOS (BYOD)

4.1 Objetivos

Establecer las normas que garanticen la seguridad de la información si se permite el uso de los dispositivos personales en el ámbito corporativo.

4.2 Puntos clave

- **Prohibición de uso de dispositivos manipulados.** Se prohíbe el uso de dispositivos *rooteados* o a los que se les ha realizado *jailbreak* ya que permiten la instalación de aplicaciones no oficiales. Por ello antes del uso de cualquier aplicación corporativa el teléfono deberá ser verificado por el departamento TIC.
- **Limitación de acceso a redes desconocidas.** Una vez tenemos las aplicaciones corporativas en uso en el teléfono móvil, es de obligado cumplimiento no conectarse a ninguna red pública que no sea de confianza. Solo si se trata de la red doméstica, la propia red móvil o la red interna, deberemos hacer uso.
- **Control de usuarios y dispositivos.** Se realizará, por parte del departamento TIC, un seguimiento sobre los usuarios y dispositivos que tengan acceso a los datos y aplicaciones de la empresa, detallando los privilegios de seguridad asignados para autorizar el acceso tanto a esos usuarios como a los dispositivos.
- **Bloqueo programado.** Se configurará el dispositivo para que se bloquee automáticamente tras un periodo de inactividad.

- **Desconexión wifi y Bluetooth.** Se desactivará en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no se estén utilizando.

5. CONTRASEÑAS

5.1 Objetivos

Con objeto de incrementar la seguridad y la privacidad en los accesos a las herramientas informáticas corporativas se hace preciso aplicar medidas respecto a las contraseñas de acceso a los equipos informáticos y cuentas.

5.2 Puntos clave

- **Características.** Debe componerse mínimo de 8 caracteres, entre los que son obligatorios:
  - carácter en mayúscula (A, B, C, D, E, F, etc);
  - carácter en minúscula (a, b, c, d, e, f, etc);
  - carácter numérico (1, 2, 3, 4, 5, etc);
  - carácter especial (¿, ¡, $, #, etc).
- **Vigencia.** Transcurridos 120 días se solicitará la renovación.
- **Cierre de sesión tras inactividad.** 5 minutos.
- **Configuración.** Deben de crearse contraseñas complejas en todas las cuentas de usuario.
- **Uso de aplicación de gestión de contraseñas.** Para los empleados que trabajen diariamente con distintas cuentas para el login, tanto en servicios de mensajería o comercios electrónicos, por ejemplo, es muy recomendable el uso de una aplicación para la gestión de credenciales de acceso. Buen ejemplo de ello es *KeePass*, de la que existe un manual de uso en el portal *FreshDesk*.