MANUAL DE RECOMENDACIONES DE CIBERSEGURIDAD DEL GRUPO REDVOISS

ENERO 2022

CONTENIDO

Almacenamiento en la red corporativa

Para poder disponer de un lugar común de trabajo donde almacenar el resultado de los trabajos individuales y poder compartir información entre los diferentes usuarios de la empresa se dispone de servidores de almacenamiento en red. En la red del Grupo Redvoiss se requiere que la información general de la empresa y de los clientes que utilicen los usuarios, e información de trabajo de los empleados almacenada en esta red corporativa se maneje con criterios de seguridad. Para ello, se deben aplicar controles de acceso a esta información con el objetivo de limitar quién puede acceder y a dónde.

El contenido de la información almacenada debe clasificar con los siguientes aspectos: tipo de información almacenada, momento de su almacenamiento y ubicación dentro de los directorios del sistema, además de las personas encargadas de la actualización de dicha información en caso de modificación. Se prestará una especial atención cuando la información haya sido catalogada como confidencial o crítica o si está sujeta a algún requisito legal.

Si la empresa requiere almacenar gran cantidad de información, deberá utilizar sistemas de almacenamiento en redes del tipo NAS (Network Attached Storage), para archivos compartidos, o SAN (Storage Area Network) de alta velocidad para bases de datos de aplicaciones. Estos sistemas presentan un volumen de almacenamiento grande, ya que unen la capacidad de múltiples discos duros en la red local como un volumen único de almacenamiento.

Objetivo del almacenamiento en la red corporativa

Los trabajadores hagan un buen uso de los servidores de almacenamiento disponibles para un óptimo tratamiento de la información. Concienciar a los empleados de la relevancia de la información corporativa del Grupo Redvoiss, para un buen desempeño de su trabajo y de la necesidad de almacenarla en un sitio centralizado para evitar duplicidades y problemas de versiones, evitar pérdidas de documentos, centralizar las copias de seguridad, compartir información para la elaboración de proyectos y documentos, etc.

Controles para aplicar el almacenamiento en la red corporativa

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a almacenamiento en la red corporativa.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** Aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** Aplica al personal técnico especializado.
- **Personas (PER):** Aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Inventario de los servidores de almacenamiento.** Informar a los empleados sobre los servidores de almacenamiento disponibles, la información que se comparte, qué datos deben almacenarse en ellos y las responsabilidades que conlleva.	☐
B	PRO	**Criterios de almacenamiento.** Informar a los empleados sobre los criterios de almacenamiento corporativos (qué se puede almacenar, quién tiene acceso y cuándo se elimina la información).	☐

NIVEL	ALCANCE	CONTROL	
B	PRO	**Clasificación de la información.** Informar al empleado sobre la necesidad de cumplir la política de clasificación de la información a la hora de almacenar y eliminar información en la red corporativa.	☐
A	PRO/TEC	**Control de acceso.** Estableces e implementas reglas de acceso que permiten llevar un control de quién tiene acceso y a qué discos/directorios.	☐
A	PRO/TEC	**Copias de seguridad.** Definir un plan de copias de seguridad en el que se detalla la información a guardar, cada cuanto tiempo se va a realizar, donde se va a almacenar y el tiempo de conservación de la copia.	☐
A	TEC	**Acceso limitado.** Permitir el acceso a los empleados solo a los repositorios necesarios para el desempeño de su trabajo.	☐
A	TEC	**Almacenamiento clasificado.** Crear carpetas organizadas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde. Asignar los permisos de acceso pertinentes según el perfil del empleado.	☐
A	TEC	**Auditoría de servidores.** Revisar periódicamente el estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.	☐
A	TEC/PER	**Cifrado de la información.** Cifrar la información crítica almacenada en los servidores.	☐

Controles necesarios para la gestión de almacenamiento en la red corporativa

- **Inventario de los servidores de almacenamiento**. Se debe poner en conocimiento de los empleados cuáles son los servidores de almacenamiento disponibles en la red corporativa, la información que se comparte, qué datos deben ser almacenados en los mismos y las responsabilidades que conlleva. Esto se deberá reflejar en la formación de los nuevos empleados y refrescarse cada cierto tiempo.

- **Criterios de almacenamiento.** Se debe elaborar una normativa que establezca que la información debe almacenarse en la red corporativa teniendo en cuenta los siguientes aspectos:
  - qué información debe o no debe almacenarse en estos directorios;
  - las personas que tienen acceso a la información y si son encargadas su actualización en caso de necesidad de modificación;
  - cuando es necesario eliminar la información por quedarse obsoleta.

- **Clasificación de la información.** El empleado debe conocer y cumplir la Política de de seguridad de información y se debe realizar clasificar la información a la hora de almacenar y eliminar información en la red corporativa. De esta forma se almacenará en la forma y lugar correctos.

- **Control de acceso**. Se debe establecer e implementar reglas de acceso que permitan llevar un control de quién tiene acceso y a qué directorios o sistemas de almacenamiento.

- **Copias de seguridad.** Ejecutar el plan de copias de seguridad, en el que se detalla la información a guardar, cada cuánto tiempo se va a realizar, dónde se va a almacenar y el tiempo de conservación de cada copia.

- **Acceso limitado**. Según lo establecido en la política de seguridad de información, se debe definir perfiles de acceso (y se asignan a los usuarios) que limitan el uso de la información, de manera que cada usuario acceda solo a los directorios necesarios para el desempeño de su actividad laboral.

- **Almacenamiento clasificado.** Se debe crear carpetas según du clasificación de seguridad para que el personal almacene la documentación donde corresponde. Se asignarán los permisos de acceso pertinentes según el perfil del empleado.

- **Cifrado de la información**. Según la política de seguridad de información, se debe

implantar procedimientos de cifrado la información crítica que se almacene en la red corporativa.

- **Auditoría de servidores.** Coordinar tiempos específicos para monitorear y revisar el estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.

Almacenamiento en el servidor de archivos y los equipos de trabajo

En el puesto de trabajo, los empleados utilizan como herramienta equipos informáticos: computadores de escritorio, laptops, tabletas, teléfonos móviles, etc. También se generan y transmiten información necesaria para el desempeño de sus funciones. Esta información a veces se almacena de manera local de forma temporal en los discos duros de estos equipos, por lo que surge la necesidad de disponer de una política que regule cómo hacerlo de forma segura. Igualmente deben regularse en forma de políticas el almacenamiento en dispositivos extraíbles, en la nube y en la red corporativa.

En el Grupo Redvoiss de debe implementar una Política de clasificación de la información. Con esta clasificación se elaborará una normativa para el tratamiento de la información crítica y sensible, que indicará cuando debe ir cifrada, cuando se ha de controlar el acceso a la misma y otras medidas de seguridad a llevar a cabo como las copias de seguridad o la destrucción de la información.

Objetivos de la gestión del almacenamiento en el servidor de archivos y los equipos de trabajo

Mantener de modo seguro la información almacenada en el servidor de archivos y de forma local, especificando reglas, criterios y procedimientos que deben seguir todos los empleados.

Controles para aplicar la gestión del almacenamiento en el servidor de archivos y los equipos de trabajo

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** El esfuerzo y los recursos necesarios para implantarlo son considerables.

Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** Aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** Aplica al personal técnico especializado.
- **Personas (PER):** Aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Qué se puede almacenar en los equipos corporativos.** Elaborar una normativa que regula el almacenamiento de información personal en los equipos corporativos.	☐
B	PRO	**Dónde guardar la información.** Informar a los empleados sobre dónde guardar la información generada en su trabajo dentro del servidores de archivos para la información de la empresa árbol de directorios del equipo.	☐
B	PRO	**No conservación de la información en discos locales pertenecientes a la empresa y clientes.** Indicar que solo se puede conservación información temporal de forma local en caso de ser corporativa y de clientes se debe transferir a los servidores de archivos indicados y eliminar del local.	☐
A	PRO/TEC	**Permanencia de la información en discos locales una vez transferida a los servidores.** El tiempo de permanencia de la información en local una vez transmitida a los servidores corporativos es inmediata. Será eliminada cualquier que sea local perteneciente al Grupo Redvoiss.	☐

A	TEC/PER	**Cifrado de la información.** En caso de tener que guardar información local. Se debe cifrar la información crítica y sensible antes de guardarla localmente.	☐
B	PER	**Conocimiento y aplicación de la normativa.** Conocer y aplicar la normativa establecida.	☐

Controles necesarios para la gestión del almacenamiento en el servidor de archivos y los equipos de trabajo

- **Qué se puede almacenar en los equipos corporativos.** Los empleados deben conocer qué solo se debe almacenar información de tipo tempral y no sensible de la empresa en los equipos locales. De igual formase debe regular el almacenamiento de información en los equipos locales, indicando la información que no debe almacenarse (documentos personales, archivos de música, fotografías, etc.).

- **Se debe prestar especial atención a los archivos descargados que posean derechos de autor**. Los empleados no almacenarán información que no haya sido aprobada por la organización.

- **Dónde guardar la información.** La normativa debe detallar dónde guardar la información derivada del trabajo dentro del árbol de directorios del equipo. Esta medida facilita la migración de esta información a servidores.

- **No conservación la información en discos locales.** Para evitar problemas de espacio en los discos duros estableceremos un periodo de tiempo de conservación de la información temporal. Transcurrido este tiempo, según la información en cuestión, se tiene que transferir a los servidores empresariales o si se elimina definitivamente.

- **Permanencia de la información en discos locales una vez transferida a los servidores**. Si la información ya se ha transferido a los servidores corporativos, se tiene que establecer que no puede tener permanencia en local para no almacenar por duplicado la información.

- **Cifrado de la información.** El empleado debe conocer cuándo y cómo utilizar el cifrado de documentación, según la Política de uso de técnicas criptográficas. Esta medida es útil en caso de fuga de información o acceso no autorizado.

- **Conocimiento y aplicación de la normativa.** Los empleados deben conocer y aplicar la normativa relativa al almacenamiento en local en sus equipos de trabajo y otras políticas relacionadas

Clasificación de la información

La información es uno de los activos principales para el Grupo Redvoiss y como tal tenemos que protegerla adecuadamente. Los activos de información pueden estar en formato digital o en otros soportes (papel, película fotográfica, etc.). En formato digital podrán ser desde ficheros de todo tipo (texto, imagen, multimedia, bases de datos, …), pasando por los programas y aplicativos que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios.
Se deben aplicar las medidas de seguridad ajustadas a cada activo de información, realizar un inventario y clasificarlos, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, aplicando para ello criterios de confidencialidad, integridad y disponibilidad. De esta forma, tener el conocimiento de la información debemos cifrar, quién puede utilizarla, quién es responsable de su seguridad, cada cuanto hacer backups, etc.

Es importante considerar que, al clasificar los activos de información, debemos establecer su ciclo de vida, que dependerá no sólo de la vida útil del soporte sino también de la vigencia de su contenido. Si el soporte caduco antes que el contenido, tendremos que regenerarlo en otro soporte. El ciclo de vida de la información determinará el momento en el cual dejará de ser útil, y por tanto cuándo tenemos que eliminarla convenientemente.

Objetivos de la clasificación de la información

Clasificar los activos de información para garantizar una eficaz gestión de su seguridad con criterios de confidencialidad, disponibilidad e integridad.

Controles para aplicar en la clasificación de la información

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a la clasificación de la información.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Inventario de la información** Elaborar un inventario detallado de los activos de información de la empresa.	☐
B	PRO	**Criterios de clasificación de la información** Determinar claramente los criterios de seguridad y clasificar los activos de información de la empresa.	☐
B	PRO	**Clasificación de la información** Etiquetar los activos de información según los criterios de seguridad establecidos.	☐
B	PRO	**Tratamientos de seguridad disponibles** Establecer una lista con todos los tratamientos de seguridad de la información disponibles en la empresa.	☐
A	TEC	**Establecer y aplicar los tratamientos que corresponden a cada tipo de información** Aplicar correctamente los tratamientos de seguridad que corresponden a cada activo información.	☐
A	TEC	**Auditorías** Realizas auditorías de comprobación	☐

Controles necesarios para la aplicación de la clasificación de la información

- **Inventario de la información.** Se debe establecer un inventario de los activos de información disponible en la empresa, considerando registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen, quienes son sus responsables, etc.

- **Criterios de clasificación de la información**. Establecer claramente los criterios de clasificación que vamos a aplicar a los activos de información. Estos deberán estar relacionados con las medidas de seguridad que plantearemos aplicar a nuestra información. Algunos de estos criterios son:

    - **Por el nivel de accesibilidad o confidencialidad:**
        - Confidencial. Accesible solo por la dirección o personal concreto
        - Interna. Accesible solo al personal de la empresa
        - Pública. Accesible públicamente.

    - **Por su utilidad o funcionalidad:**
        - información de clientes y proveedores
        - información de compras y ventas
        - información de personal y gestión interna
        - información sobre pedidos y procesos de almacén

    - **Por el impacto por robo, borrado o pérdida:**
        - daño de imagen
        - consecuencias legales
        - consecuencias económicas
        - paralización de la actividad

- **Clasificación de la información.** Asignar a cada tipo de información una etiqueta según los criterios de clasificación establecidos.
- **Tratamientos de seguridad disponibles.** Elaborar un listado con todos los tratamientos de seguridad de los que dispone la empresa, tales como herramientas de cifrado, sistemas de copias de seguridad, sistemas de control de accesos, etc.

- **Establecer y aplicar los tratamientos que corresponden a cada tipo de información.** Una vez clasificada la información, debemos asignar y aplicar los tratamientos de seguridad oportunos para cada tipo de información. Entre estos tratamientos, podríamos

contemplar los siguientes:

- limitar el acceso a las personas o grupos correspondientes
- cifrar la información
- realizar copias de seguridad
- medidas específicas como las reflejadas en las políticas de privacidad de datos
- información sujeta a acuerdos de confidencialidad concretos
- control del acceso y/o modificación de la información

- **Auditorías.** realizar periódicamente auditorías de seguridad, que certifiquen que se aplican los tratamientos estipulados para proteger nuestra información.

Gestión del correo electrónico

El correo electrónico, es una herramienta de comunicación imprescindible para el funcionamiento del Grupo Redvoiss. Sus beneficios son evidentes: accesibilidad, rapidez, posibilidad de enviar documentos adjuntos, etc., aunque cuando se creó, no se hizo pensando en sus aplicaciones actuales ni en la seguridad.

Como toda herramienta de comunicación corporativa es necesario definir su uso correcto y seguro, ya que, además de abusos y errores no intencionados en su uso que puedan causar perjuicio en la empresa, el correo electrónico se ha convertido en uno de los medios que utilizan los ciberdelincuentes para llevar a cabo sus ataques.

Los empleados pueden enviar documentos confidenciales a quien no deberían por error, desvelar, sin querer, la dirección del correo electrónico (que es un dato personal) de clientes o usuarios, o utilizar su correo corporativo para usos no permitidos.

También es habitual que a los buzones corporativos llegue spam, correos de phishing que intentan robar credenciales o correos que suplantan entidades o personas. En estos casos utilizan técnicas de ingeniería social para conseguir sus fines maliciosos, por ejemplo: infectarnos, robar credenciales o que les demos datos confidenciales. En un correo malicioso tanto el remitente como el asunto, el cuerpo, los adjuntos o los enlaces que contiene, pueden estar diseñados para engañar al receptor del mensaje. Para evitar caer en la trampa de los ciberdelincuentes debemos además de utilizar medios tecnológicos (antivirus, antimalware, antispam, etc.), concienciar a nuestros empleados para que sepan distinguir estos mensajes.
Para evitar los riesgos que conlleva el uso del correo corporativo debemos concienciar a nuestros empleados para que hagan un uso seguro del mismo e informarles de las normas que

regulan las condiciones y circunstancias en las que puede utilizarse, así como las posibles sanciones y acciones a tomar en caso de detectarse un mal uso.

Objetivos de la gestión del correo electrónico

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.

Controles para aplicar la gestión del correo electrónico

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a almacenamiento en la red corporativa.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** Aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** Aplica al personal técnico especializado.
- **Personas (PER):** Aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Normativa de uso de correo electrónico** Disponer de una normativa referente al uso del correo electrónico que el empleado aceptará al incorporase a su puesto de trabajo.	☐

NIVEL	ALCANCE	CONTROL	
B	TEC	**Antimalware y antispam** Instalar y activar aplicaciones antimalware y filtros antispam tanto en el servidor como en los clientes de correo.	☐
A	TEC	**Cifrado y firma digital** Instalar una tecnología de cifrado y firma digital que se pueda usar con el correo electrónico para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.	☐
A	TEC	**Desactivar el formato HTML, la ejecución de macros y la descarga de imágenes en los clientes de correo electrónico** Desactivar el formato HTML, la ejecución de macros y la descarga de imágenes para una protección adicional de las cuentas de correo electrónico.	☐
B	TEC/PER	**Ofuscar las direcciones de correo electrónico** No publicar las direcciones de correo corporativas, en páginas web ni en redes sociales sin utilizar técnicas de ofuscación.	
B	PER	**Uso apropiado del correo corporativo** Nunca usar el correo corporativo con fines personales y el contenido cumple las normas marcadas por la empresa.	☐
B	PER	**Contraseña segura** Usar una contraseña segura para acceder al correo electrónico.	☐
B	PER	**Correos sospechosos** Sospechar de la autenticidad del correo cuando el mensaje: presenta cambios de aspecto, contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual o solicitar credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.).	☐

NIVEL	ALCANCE	CONTROL	
B	PER	**Identificación del remitente** Identificar los remitentes antes de abrir un correo electrónico. Si sospechas que ha sido suplantado contactar con el remitente por otro medio para confirmarlo.	☐
B	PER	**Análisis de adjuntos** Analizar cuidadosamente los adjuntos de correos de remitentes desconocidos antes de abrirlos. Si se sospecha de su autenticidad, no se debe descargar ni abrir.	☐
B	PER	**Inspección de enlaces** Examinar atentamente los enlaces incluidos en los correos antes de acceder a ellos.	☐
B	PER	**No responder al spam (correo basura)** Nunca responder al correo basura. Lo agregar a la lista de spam y eliminar.	☐
B	PER	**Utilizar la copia oculta (BCC o CCO)** Utilizar la copia oculta cuando se envían correos a múltiples direcciones.	☐
B	PER	**Reenvío de correos** En caso de necesitar el reenvío de algún correo corporativo a una cuenta personal, se debe solicitar previamente a la dirección.	☐
B	PER	**Evitar las redes públicas** No consultar el correo corporativo si se está conectado a redes públicas como wifi de hoteles o aeropuertos.	☐

Controles necesarios para la gestión del correo electrónico

- **Normativa de uso de correo electrónico.** El Grupo Redvoiss, dispondrá de una normativa referente al uso del correo electrónico que el empleado aceptará al incorporase a su puesto de trabajo. Se informará de la prohibición del uso del correo corporativo con fines personales que no tengan que ver con la empresa. El contenido del correo deberá cumplir con la normativa y su uso inadecuado podrá conllevar sanciones. El correo

corporativo puede ser supervisado por la dirección de la empresa, incluyendo una cláusula en la normativa que firma el empleado.

- **Antimalware y antispam.** Se debe instalar aplicaciones antimalware y activar los filtros antispam tanto en el servidor como en el cliente de correo según la Política gestión de antivirus y antimalware. Estos filtros permitirán que los correos maliciosos sean identificados y no lleguen a la bandeja de entrada evitando así su posible apertura.

- **Cifrado y firma digital.** De ser el caso, se debe instalar una tecnología de cifrado y firma digital para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.

- **Desactivar el formato HTML**, la ejecución de macros y la descarga de imágenes. El formato HTML permite utilizar colores, negritas, enlaces, etc. También permite incluir un lenguaje de programación denominado JavaScript. Este lenguaje puede ser usado con fines ilícitos, por ejemplo, para verificar que nuestra cuenta de correo es válida o para redirigirnos a un sitio web malicioso. Por ello es más seguro tenerlo desactivado. Como seguridad complementaria también se deberían deshabilitar las macros y las descargas de imágenes.

- **Ofuscar las direcciones de correo electrónico.** No se deben publicar las direcciones de correo corporativas en páginas web, ni en redes sociales, sin utilizar técnicas de ofuscación. De lo contrario, esas cuentas pueden ser captadas para incluirlas en listas de envío de spam. Técnicas que puedes utilizar:

    - crear una imagen con la dirección de correo que quieras publicar y utiliza la imagen en lugar de introducir el correo como texto;
    - reemplazar '@' y '.' por texto; de esta forma, nombre@miempresa.com se sustituiría por nombrearrobamiempresapuntocom.

- **Uso apropiado del correo corporativo**. El empleado debe conocer y aceptar la normativa relativa al uso del correo corporativo.

- **Contraseña segura.** Todas las cuentas deben utilizarse con contraseñas de acceso de acuerdo con la Política de contraseñas, se recomienda:

    - usar una contraseña segura para evitar accesos no autorizados;
    - utilizar doble factor de autenticación para las cuentas críticas;

- al acceder al correo a través desde una interfaz web, nunca se marcará la opción de recordar 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 hacer algo no habitual;
  - se soliciten credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.)

- **Identificación del 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, …) sospechas que se ha podido suplantar su identidad, se debe 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 se reciba un correo no deseado, no responder 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 corporativo, desde conexiones públicas (la wifi de una cafetería, el computador de un hotel, etc.) de acuerdo con la Política gestión de acceso desde redes externas por VPN y WIFI, 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.

Copias de seguridad (backups)

Los medios de almacenamiento son parte fundamental de los activos de la información para el Grupo Redvoiss. Estos dispositivos pueden verse involucrados en situaciones como robos, incendios, inundaciones, fallos eléctricos, rotura o fallo del dispositivo, virus, borrados accidentales, etc. En estos casos es imposible acceder a nuestra información, llegando a ponerse en peligro la continuidad de nuestro negocio. Para el Grupo Redvoiss, el fundamental tener un inventario de activos de información y una clasificación de estos en base a su criticidad para el negocio. El objetivo de esta clasificación es tener un registro de todo el software y los datos imprescindibles para la empresa de manera que sirva para determinar la periodicidad de los backups y su contenido.

Es importante considerar que es responsabilidad del equipo técnico de TI, el identificar, realizar los backups y definir el procedimiento para hacer las copias de seguridad y restaurarlas, tomando en cuenta los siguientes aspectos:

- de qué hacer copia,
- el tipo de copia,
- el programa necesario,
- los soportes,
- la periodicidad,
- la vigencia,
- su ubicación,
- y las pruebas de restauración.

Así mismo se llevar un control de los soportes utilizados, vigilar que sólo tiene acceso personal autorizado y que se destruyen los soportes de forma segura, en caso de tener que desecharlos. Los mismos criterios de seguridad serán aplicables en caso de hacer copias en la nube o en proveedores externos.

Objetivos de las copias de seguridad (backups)

Verificar que se realizan copias de seguridad que garantizan la continuidad de negocio.

Controles para aplicar a las copias de seguridad (backups)

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a copias de seguridad.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Inventario de activos de información** Mantener el inventario de activos de información (software, datos, soportes, responsables, ubicación…) y los clasificas para identificar los necesarios (críticos) para reanudar el negocio en caso de desastre o incidente grave.	☐
B	PRO	**Control de acceso** Controlar el acceso a las copias de seguridad (sólo personal autorizado).	☐
B	PRO/TEC	**Copias de seguridad de la información crítica** Hacer copias de seguridad de la información crítica corporativa, la exigida por la ley y la establecida en los contratos.	☐
B	PRO/TEC	**Periodicidad de las copias de seguridad** Las copias de seguridad se realizan cada 15 días y dependiendo a solicitud de clientes.	☐
B	PRO/TEC	**Tipo de copia apropiada** Hacer copias de seguridad completa, incremental o diferencial (elegir de acuerdo a las capacidades).	☐

NIVEL	ALCANCE	CONTROL	
B	PRO/TEC	**Caducidad de las copias de seguridad** Conservar las copias de seguridad durante 5 años.	☐
A	PRO/TEC	**Ubicación de las copias de seguridad** Guardar al menos una copia completa fuera de la organización. Además de guardar las copias de seguridad en una caja ignífuga y bajo llave.	☐
A	PRO/TEC	**Copias en la nube** Tomar las medidas de seguridad (firmar SLAs con el proveedor, cifrar las copias, comprobar la confidencialidad de los canales de transmisión) necesarias si almacenas tus copias en la nube.	☐
B	PRO/TEC	**Procedimientos de copia y restauración** Elaborar y aplicar los procedimientos de copia y restauración, revisándolos anualmente y con cada cambio importante en los activos de información.	☐
B	TEC	**Comprobar que las copias están bien realizadas y que pueden restaurarse** Comprobar cada 6 meses la fiabilidad de las copias verificando que pueden restaurarse.	☐
A	TEC	**Soporte de las copias de seguridad** Antes de hacer la copia revisar que el soporte es el adecuado (tasa de transferencia, capacidad, …) y que está en buen estado.	☐
B	TEC	**Control de los soportes de copia** Etiquetar los soportes para realizar las copias de seguridad y llevas un registro de los soportes sobre los que se ha realizado alguna copia.	☐
B	TEC	**Destrucción de soportes de copia** Establecer que cuando se desechan los soportes utilizados para copias de seguridad, sean destruidos de forma segura.	☐
B	PER/TEC	**Cifrado de las copias de seguridad** Cifrar las copias de seguridad que contienen información confidencial y la que subes a la nube. **Mínimo cifrado 256 bits, preferible 2048 bits.**	☐

Controles necesarios para las copias de seguridad (backups)

Los puntos clave de esta política son:

- **Inventario de activos de información**. Se debe tener actualizada e identifica toda la información necesaria para reanudar el negocio en caso de desastre o de incidente grave. Se incluirá el software necesario y los datos críticos, los dispositivos que lo albergan, los responsables, la ubicación, etc.

- **Control de acceso**. Las copias de seguridad han de estar sometidas a un control de acceso restringido al personal autorizado.

- **Copias de seguridad de la información crítica**. verificar el cumplimiento especifico exigido para las copias de seguridad de la información crítica corporativa y de la establecida en los contratos con terceros.

- **Periodicidad de las copias de seguridad.** Se debe fijar la frecuencia para hacer las copias de seguridad teniendo en cuenta:

    - la variación de los datos generados;
    - el coste de almacenamiento;
    - y las obligaciones legales, por ejemplo, contratos con terceros y en función a las leyes de protección de datos. En especial consideración a las empresas con tratamiento especial de datos de carácter personal, se debe establecer procedimientos de actuación para la realización de copias de respaldo.

- **Tipo de copia apropiada.** Determinar qué tipo de copia de seguridad es la idónea estimando los recursos y tiempo necesarios para llevarlas a cabo:

    - **completa:** se copian todos los datos a un soporte;
    - **incremental:** sólo se graban los datos que han cambiado desde la última copia;
    - **diferencial:** se copian los datos que han cambiado desde la última copia completa.

- **Caducidad de las copias de seguridad.** Se debe decidir cuánto tiempo conservar las copias en función de:

    - si la información almacenada sigue vigente;
    - la duración del soporte en el que realizan las copias;
    - la necesidad de conservar varias copias anteriores a la última realizada.

- **Ubicación de las copias de seguridad.** Es necesario buscar un lugar adecuado para guardar las copias, con los siguientes criterios:

- cuenta con al menos una copia fuera de la organización;
- no guardar backups con datos de carácter personal (datos de clientes o de empleados, por ejemplo) en casa;
- contratar servicios de guarda y custodia según los datos que contienen.

- **Copias en la nube.** En el caso de copias en la nube, de debe tomar las siguientes precauciones para garantizar la seguridad de la información:

  - cifrar la información confidencial antes de realizar la copia;
  - firma Acuerdos de Nivel de Servicios (SLA) con el proveedor, que garanticen la disponibilidad, integridad, confidencialidad y control de acceso a las copias;
  - considera el ancho de banda que necesitas para subir y bajar las copias.

- **Procedimientos de copia y restauración.** Se debe elaborar y aplicar procedimientos que describan cómo hacer las copias y cómo restaurarlas. De esta forma se minimiza el tiempo necesario de recuperación de los datos en caso de necesitar una restauración. Se han de revisar anualmente y con cada cambio importante del inventario de activos de información.

- **Comprobar que las copias están bien realizadas y que pueden restaurarse.** Fijar una periodicidad para realizar pruebas de restauración para garantizar que la información necesaria para la continuidad de negocio puede ser recuperada en caso de desastre.

- **Soporte de las copias de seguridad.** Establecer dónde hacer las copias teniendo en cuenta los siguientes aspectos:

  - coste, fiabilidad, tasa de transferencia y capacidad de los distintos soportes: discos duros externos, USB, cintas, DVD y la nube;
  - utilizar soportes que no estén obsoletos o en mal estado.

- **Control de los soportes de copia.** Se debe etiquetar e identificar los soportes dónde se realizan las copias de seguridad de manera que se pueda llevar un registro de los soportes sobre los que se ha realizado alguna copia. Así en el caso de tener que recuperar una información concreta, agilizaremos el proceso al poder consultar fácilmente en qué soporte se ha almacenado.

- **Destrucción de soportes de copia**. Cuando se desechen los soportes utilizados para

copias de seguridad, deben ser destruidos de forma segura. Asegurar que esta información nunca volverá a ser accesible para evitar posibles accesos malintencionados.

- **Cifrado de la información** Cifrar la información confidencial y la que requiera de almacenamiento en la nube. De esta manera protegemos los datos en caso de robo de información o accesos no autorizados.

Borrado seguro y gestión de soportes

Para el Grupo Redvoiss, se toma en consideración que en algún momento luego de cumplir su ciclo de vida, la información deja de ser necesaria para la organización y es necesario destruirla de forma segura. Esta opción es indispensable, para que la información no vuelva a ser accesible y cumplir con la Ley de Protección de Datos, más aún cuando contenga datos de carácter personal.

De igual forma se debe considerar, que también se debe utilizar el borrado seguro cuando se requiere:

- reutilizar un soporte:
  - que ya contiene datos corporativos;
  - que no funciona correctamente;

- o se requiere deshacer de un soporte que se ha quedado obsoleto.

En el caso de que la información esté en soportes no electrónicos (papel, negativos fotográficos, radiografías, cintas magnéticas, etc.) es necesario usar una trituradora para deshacerse de la información. En caso contrario podría llegar a manos de terceros y utilizarse de forma perjudicial para la empresa.

Por otro lado, en caso de contratar a terceros para la destrucción de datos o de los soportes, se debe elegir la destrucción certificada si se trata de (o si contienen) datos personales o confidenciales. Esta opción asegura la destrucción de la información con las máximas garantías de seguridad y confidencialidad, desde la recogida del material documental hasta su destrucción física y eliminación final.

Objetivos para el borrado seguro y gestión de soportes

Establecer normas para el borrado seguro de la información obsoleta y para destrucción de soportes acorde a las necesidades de la empresa.

Controles para aplicar el borrado seguro y gestión de soportes

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a borrado seguro y gestión de soportes.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Inventario de activos** Realizar un seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio.	☐

NIVEL	ALCANCE	CONTROL	
B	PRO/TEC	**Gestión de soportes** Supervisar los dispositivos que almacenan información corporativa, en particular aquellos que se utilizan para realizar copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, reparación, sustitución, etc.	☐
A	PRO/TEC	**Eliminación de la información en soportes no electrónicos** Utilizar el proceso de triturado para destruir la información de los soportes no electrónicos (papel y soportes magnéticos).	☐
A	PRO/TEC	**Eliminación de la información para la reutilización de soportes electrónicos** Optar por el proceso de sobreescritura cuando quieres reutilizar un soporte todavía en buen estado.	☐
A	PRO/TEC	**Eliminación de la información antes de deshacernos de soportes electrónicos** Usar el proceso de desmagnetización o de destrucción física antes de desechar el soporte de almacenamiento.	☐
A	PRO/TEC	**Borrado de información en otros dispositivos** Eliminar la información en teléfonos móviles, impresoras, GPS, etc. (memoria y tarjetas) antes de deshacernos de ellos.	☐
A	TEC	**Documentación de las operaciones de borrado realizadas** Elegir una herramienta de borrado que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado.	☐

NIVEL	ALCANCE	CONTROL	
A	TEC	**Destrucción certificada** Utilizar un servicio de destrucción certificada para garantizar la destrucción de datos confidenciales o para cumplir un acuerdo con otra empresa o con leyes de protección de datos.	☐

Controles necesarios para el borrado seguro y gestión de soportes

- **Inventario de activos:** tendremos que realizar un seguimiento de los dispositivos que están en funcionamiento (CD, DVD, Flash USB, discos magnéticos, tarjetas de memoria…), las personas o departamentos responsables de esos dispositivos, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio.

- **Gestión de soportes:** supervisaremos los dispositivos que almacenan información corporativa, en particular los que se usan para realizar las copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, repa-ración, sustitución, etc.

- **Eliminación de la información:**

    - **En soportes no electrónicos y soportes magnéticos:** Para eliminar la información que ya no se considera necesaria para la organización en este tipo de soportes (documentos impresos, CD, DVD, cintas magnéticas, radiografías, etc.) se debe utilizar la opción de triturado como modo seguro de eliminación.

    - **Para la reutilización de soportes electrónicos:** para reutilizar un soporte que ya contiene datos, se debe utilizar la opción de sobreescritura para garantizar un borrado total de la información. La sobreescritura se puede utilizar en todos los dispositivos regrabables (discos duros, pendrives o dispositivos USB, etc.) siempre que el dispositivo no esté dañado.

    - **Antes de deshacerse de los soportes electrónicos:** si se requiere el desechar de algún soporte de almacenamiento, porque ya no funcione o porque se haya quedado obsoleto, se debe utilizar los métodos de desmagnetización o destrucción física. Cualquiera de estos dos métodos imposibilita la reutilización del dispositivo.

- **Prestar una especial atención cuando se requiere el deshacerse de dispositivos móviles (smartphones, tabletas, etc.) y dispositivos que almacenan información de uso (impresoras, GPS, etc.)** ya que también pueden contener información empresarial confidencial.

- **Documentación de las operaciones de borrado realizadas**: al seleccionar una herramienta de borrado, elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado.

- **Destrucción certificada:** existe la opción de contratar una empresa que realice una destrucción certificada. Esta empresa se encargará de llevar a cabo el proceso de eliminación de la información garantizando la gestión y control de recogida, transporte y destrucción del material confidencial. Después de llevar a cabo la destrucción, la empresa emite un certificado que garantiza la validez de todo el proceso. Esta alternativa es muy útil si queremos garantizar la destrucción de datos confidenciales y en el caso de que exigencia por un contrato o acuerdo con otra empresa.

Gestión de logs

En el Grupo Redvoiss, es importante la gestión de los sistemas registran la actividad de los usuarios y de sus procesos internos (login/logout, origen, tiempo de actividad, acciones, conexiones, …) en registros de eventos o logs. La información de estos registros es esencial para elaborar informes de gestión y para monitorización. Entre los eventos que los distintos sistemas registran están, por ejemplo: el inicio/fin de sesión, el acceso y modificación de ficheros y directorios, cambios en las configuraciones principales, lanzamientos de programas, etc.

Los registros de actividad de los distintos sistemas y equipos son los datos a partir de los cuales es posible no sólo detectar fallos de rendimiento o mal funcionamiento, sino también detectar errores e intrusiones. Con ellos se alimentan sistemas de monitorización que convenientemente configurados pueden generar alertas en tiempo real. Por otra parte, facilitan el análisis forense para el diagnóstico de las causas que originan los incidentes. Por último, son necesarios para verificar el cumplimiento de ciertos requisitos legales o contractuales durante las auditorías.

Objetivos de la gestión de logs

Determinar los eventos más significativos dentro de nuestros sistemas de información que han de ser registrados, y en qué modo ha de efectuarse dicho registro. Además de, establecer

mecanismos de monitorización que permitan la detección de intrusiones, errores y situaciones anómalas o potencialmente peligrosas.

Controles para aplicar en la gestión de logs

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a la gestión de logs.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Qué actividad debe ser registrada** Analizar qué eventos producidos en los sistemas de información se necesitan registrar.	☐
B	PRO	**Información relevante incluida en el registro** Determinar para cada tipo de suceso la información más significativa que se debe almacenar.	☐
B	PRO	**Formato de la información registrada** Detallar el formato de los *logs* para facilitar su posterior análisis.	☐
A	TEC	**Elección del mecanismo de registro** Seleccionar el sistema de registro más apropiado para la empresa.	☐

B	TEC	**Protección y almacenamiento** Proteger convenientemente la información registrada en los *logs*.	☐
B	TEC	**Sincronización del reloj** Revisar la correcta sincronización temporal de todos los dispositivos.	☐
B	TEC	**Sistemas de monitorización y alerta** Configurar los sistemas de monitorización de eventos para generar en tiempo real alertas ante posibles errores y comportamientos anómalos.	☐

Controles necesarios para en la gestión de logs

- **Qué actividad debe ser registrada.** Para obtener la información crítica sobre el funcionamiento de los activos de información, se debe analizar la actividad relevante que interesa registrar. Se debe considerar registrar, entre otros, los siguientes eventos:
    - acceso, creación, borrado y actualización de información confidencial;
    - inicio y fin de conexión en la red corporativa;
    - inicio y fin de ejecución de aplicaciones y sistemas;
    - inicio y fin de sesión de usuario en aplicaciones y sistemas; intentos de inicio de sesión fallidos;
    - cambios en las configuraciones de los sistemas y aplicativos más importantes;
    - modificaciones en los permisos de acceso;
    - funcionamiento o finalización anómalos de aplicativos;
    - aproximación a los límites de uso de ciertos recursos físicos:
        - capacidad de disco;
        - memoria;
        - ancho de banda de red;
        - uso de CPU;
    - indicios de actividad sospechosa detectada por antivirus, Sistemas de Detección de Intrusos (IDS), etc.;
    - transacciones relevantes dentro de los aplicativos.

- **Información relevante incluida en el registro**. Se debe identificar que elementos de información son más útiles, que deben ser incluidos en los distintos registros. Los más habituales son:
    - identificador del usuario que realiza la acción;
    - identificación del elemento sobre el que se realiza la acción (ficheros, bases de

datos, equipos, etc.);
- identificación de dispositivos, ya sea a través de sus direcciones IP, direcciones MAC, etc.;
- identificación de protocolos;
- fecha y hora de ocurrencia del evento;
- tipología del evento.

- **Formato de la información registrada.** tener un formato de registro que ayude en la medida de lo posible a posteriores lecturas y análisis.

- **Elección del mecanismo de registro.** elegir un sistema de gestión de logs apropiado a nuestra política. Posteriormente será necesario disponer y configurar las herramientas de monitorización y registro adecuadas para implantarlo.

- **Protección y almacenamiento.** Asegurarse de que la información de registro esta convenientemente almacenada para protegerla de accesos indebidos. Es conveniente incorporar esta información a los sistemas de copia de seguridad, para poderla recuperar en caso de pérdida.

- **Sincronización del reloj**. Se debe asegurar de que todos los sistemas están sincronizados correctamente, de este modo garantizaremos el correcto registro temporal de los eventos más relevantes.

- **Sistemas de monitorización y alerta.** Paralelamente al registro de los eventos más significativos, utilizaremos los sistemas de monitorización para que nos alerten en tiempo real de posibles errores y comportamientos anómalos, tales como:

  - proximidad de alcanzar los límites en la utilización de los recursos físicos hardware;
  - finalización o comportamientos anómalos de programas;
  - comportamientos anómalos en la red;
  - cambios en configuraciones críticas;
  - picos de rendimiento anómalos en los sistemas y redes.

Actualizaciones y parches de software

Todo software es susceptible de necesitar actualizaciones por motivos de seguridad, esto incluye el firmware de los equipos electrónicos, los sistemas operativos y aplicaciones informáticas e incluso los propios programas antimalware. Los fabricantes de software lanzan actualizaciones y parches que mejoran y añaden nuevas funcionalidades, o que corrigen errores y agujeros de seguridad. En el Grupo Redvoiss es prioridad tener mantenido convenientemente y actualizados nuestros equipos y aplicaciones, de forma contraria estaríamos expuestos a todo tipo de riesgos. Los sistemas no actualizados, son aprovechados por los delincuentes para introducirse en ellos y dejarlos inactivos, infectarlos (con lo que serían menos eficientes), aprovechar su capacidad de proceso para crear botnets con fines delictivos y robar todo tipo de datos (credenciales de acceso, datos confidenciales, etc.).

Es importante estar conscientes sobre la necesidad de mantener permanentemente actualizado y parcheado todo nuestro software. Tenemos en cuenta que existen aplicaciones que incluyen sistemas de actualizaciones automáticas que es recomendable aplicar. Y en los casos de actualización manual, se toman en cuenta que las fuentes de dónde obtenemos el software, sean de confianza. En los casos en lo que recibamos servicios subcontratados de terceros, también exigiremos que el software este convenientemente actualizado. Todo el software tiene un ciclo de vida, por lo que llegado el momento puede quedar obsoleto y sin soporte oficial por parte del fabricante. En ese momento es un blanco fácil para los ciberdelincuentes (sobre todo si estamos conectados a internet) y deberíamos dejar de utilizarlo.

Objetivos de la actualizaciones y parches de software

Revisar la existencia de actualizaciones y parches de seguridad para nuestro software y elaborar procedimientos que permitan que tales actualizaciones y parches sean instalados en nuestros equipos de forma segura y controlada.

Controles para aplicar a las actualizaciones y parches de software

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a actualizaciones de software.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Determinar el software qué debe ser actualizado** Realizar un listado del software existente en la empresa para incluirlo en el plan de actualizaciones.	☐
B	TEC	**Determinar cuándo y qué actualizaciones instalar** Revisar las características y los requisitos de las actualizaciones y parches antes de instalarlos.	☐
A	TEC	**Probar las actualizaciones** Analizar y contrastar en un entorno de pruebas las actualizaciones que deseas instalar.	☐
A	TEC	**Deshacer los cambios** Contar con mecanismos y procedimientos para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente.	☐
A	TEC	**Herramientas de diagnóstico y actualización** Utilizar herramientas de autodiagnóstico para detectar software no actualizado en tus equipos.	☐
B	TEC	**Configuración de un sistema de alertas** Tener configurado un sistema de alertas para recibir avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad.	☐
B	TEC	**Registro de actualizaciones** Registrar cada una de las actualizaciones y parches que instalas.	☐

Controles necesarios para las actualizaciones y parches de software

- **Determinar el software qué debe ser actualizado**. Se debe realizar un inventario de todo el software y el firmware instalado, ya que pueden descubrirse errores o mejoras de funcionalidad. Para corregir dichos errores y garantizar un comportamiento óptimo debemos instalar, en cuando tengamos conocimiento de ellos, las correspondientes actualizaciones y parches de seguridad.

- **Determinar cuándo y qué actualizaciones instalar.** El equipo técnico de TI, debe determinar el momento en que ejecutar las actualizaciones para no interferir con las operaciones de la empresa. Aunque los principales programas comerciales disponen de funcionalidades de actualización automática, cabe la posibilidad de que tengamos software instalado que no disponga de estas opciones de actualización. En este caso usaremos los canales de alerta y los procedimientos oportunos para detectar e instalar las actualizaciones correspondientes. Antes de su instalación consideraremos la utilidad de las nuevas mejoras y la gravedad los errores que subsanan, así como los requisitos hardware/softwares necesarios.

- **Probar las actualizaciones**. Se debe instalar actualizaciones provenientes de fuentes confiables. No obstante, se debe sopesar la necesidad de disponer de un entorno de pruebas o preproducción donde instalar y probar las actualizaciones, de este modo se debe verificar que su funcionamiento es el esperado. Es obligatorio realizarlo así en las actualizaciones de aplicaciones críticas instaladas en servidores (por ejemplo: CMS, servidores web, servidores de correo, etc.).

- **Deshacer los cambios.** Antes de aceptar la instalación de una actualización, se debe considerar la forma de deshacer los cambios realizados. Así si el comportamiento del software actualizado no responde a lo esperado podremos volver a la situación anterior. Siempre es recomendable disponer antes de cualquier cambio de copias de seguridad recientes localizadas y probadas.

- **Herramientas de diagnóstico y actualización.** Existen herramientas que revisan si el software de nuestros equipos está actualizado o no. Una vez detectadas las actualizaciones pendientes, podemos proceder a su instalación en todos los equipos de manera centralizada. Esto puede ser útil en entornos con muchos equipos en los que queremos que el software instalado sea homogéneo y esté especialmente controlado.

- **Configuración de un sistema de alertas**. Configurar un sistema de alertas para

recopilar avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad del software utilizado. Estas alertas pueden ser de varios tipos:

- suscripciones a boletines genéricos sobre avisos y vulnerabilidades en la red.
- suscripciones a boletines específicos sobre actualizaciones y novedades acerca de los productos y servicios software que utilizados;
- seguimiento en redes sociales de las publicaciones especializadas en ciberseguridad;
- revisión periódica de medios y fuentes especializados;
- configuración de sistemas de avisos RSS.

- **Registro de actualizaciones.** Realizar un registro de las actualizaciones que se han instalado en nuestros sistemas. De esta forma poder tener en todo momento un conocimiento exhaustivo del software operativo en nuestros equipos.

Gestión de aplicaciones permitidas

En el Grupo Redvoiss, consideramos que las normas de protección de la propiedad intelectual, son parte fundamental del cumplimiento en todo momento y por ello solo ocupamos software legal. Estamos conscientes que el uso de software pirata o adquirido de forma fraudulenta podría conllevar sanciones económicas y penales. Además, la instalación y uso de software ilegal en algún dispositivo incrementa los riesgos de infección por malware.

Por otra parte, para evitar fugas de información y garantizar la privacidad de los datos de carácter personal, la empresa debe determinar y controlar qué software está autorizado para el tratamiento de la información dentro de la empresa. Cualquier incidente de seguridad puede repercutir en la imagen de la compañía.

Para hacer cumplir esta política la empresa cuenta con:

- un listado de software autorizado;
- un repositorio del software autorizado y un registro de licencias;
- aplicará las sanciones disciplinarias derivadas del incumplimiento de la política.

Para ello, en caso del incumplimiento, es deber el identificar a los responsables para realizar las actualizaciones del software y las auditorías.

Objetivos de la gestión de aplicaciones permitidas

Controlar que siempre se usa software autorizado en la empresa, y que ha sido adquirido de forma legal.

Controles para aplicar a la gestión de aplicaciones permitidas

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a aplicaciones permitidas. Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Registro de licencias** Mantener un registro actualizado de las licencias disponibles del software autorizado.	☐
B	PRO	**Competencia para la instalación, actualización y borrado** Nombrar y autorizar al personal técnico que se encargará de la instalación, actualización y eliminación del software de los equipos de la empresa.	☐
B	PRO	**Sanciones por usos no autorizados**	☐

		Informar al personal de la empresa de las sanciones derivadas del uso no autorizado de software.	
B	PRO/TEC	**Repositorio de software** Mantener un repositorio donde se encuentra todo el software autorizado y sus correspondientes credenciales de instalación.	☐
A	PRO/TEC	**Auditoria de software instalado** Analizar cada 3 meses que el software instalado en cada uno de los equipos de los usuarios está autorizado y tiene licencia.	☐
B	PER	**Autorización y licencia del software** Utilizar en todos los dispositivos que utilizas software autorizado y que dispone de las correspondientes licencias de uso.	☐
B	PER	**Política de copias de software** No realizar copias del software puesto a disposición, sin el debido consentimiento.	☐

Controles necesarios para la gestión de aplicaciones permitidas

- **Registro de licencias.** Se debe saber qué software dispone la organización y se debe tener un registro actualizado de licencias. En dicho registro se almacenará al menos la siguiente información:

    - nombre y versión del producto
    - autor
    - fecha de adquisición y vigencia de la licencia
    - tipo de licencia
    - número de usuarios permitidos por licencia
    - número de licencias adquiridas por cada software
    - facturas o comprobantes de compra
    - ubicación física del producto

- **Competencia para la instalación, actualización y borrado.** Para asegurar una configuración óptima en los equipos, se debe instalar únicamente por el personal técnico indicado pueda instalar, actualizar y eliminar software. En los casos en los que no se disponga de dicho personal técnico en el momento o este sea externo, se debe documentar y notificar la autorización y la operativa para instalar, actualizar, revisar y eliminar software legal de forma autónoma, para ello se deberá utilizar una cuenta de

administrador diferente a la del usuario habitual. En ningún caso debe permitirse la instalación ni la actualización de software a través de enlaces de webs o correos cuyo origen no sea completamente seguro. Por último, remarcar que además de ser legal, el software instalado en los equipos debe estar correctamente actualizado.

- **Sanciones por uso de software no autorizado.** Es importante documentar y dar a conocer las posibles sanciones disciplinarias por el uso de software ilegal o no autorizado. Además, se notificará la posibilidad de acarrear con responsabilidades civiles y penales según la legislación vigente en cada momento en materia de protección de la propiedad intelectual. Con esta medida conseguimos concienciar a la plantilla sobre las consecuencias de utilizar software ilegal.

- **Repositorio de software.** Para poder instalar el software rápidamente se debe determinar las localizaciones donde estará ubicado, así como sus claves de activación, números de serie, licencias, etc. Además, puede ser conveniente registrar metódicamente quien accede a dichos repositorios.

- **Auditoria de software instalado**. La organización debe reservarse el derecho de auditar o inspeccionar en cualquier momento los equipos de los usuarios para verificar que se cumple esta política.

- **Autorización y licencia del software.** Se debe garantizar en todo momento que los programas instalados en cualquier dispositivo corporativo (se incluyen los dispositivos BYOD. Verificar si están debidamente autorizados y que disponen de las licencias necesarias. Es aconsejable además que los empleados lean y comprendan los términos y condiciones de uso de dichas licencias De este modo de cumplir con la Ley de Propiedad Intelectual.

- **Política de copias de software.** Se debe garantizar lo especificado en las licencias de uso no se debe permitir que los empleados realicen copias del software disponible sin el debido consentimiento.

Protección del puesto de trabajo

La gestión de la información en el Grupo Redvoiss, se realiza fundamentalmente desde el puesto de trabajo, tanto desde dispositivos tecnológicos como de forma más tradicional (papel, teléfono, …). De ahí la importancia de concienciar a los empleados y exigir el cumplimiento de ciertas normas para la seguridad en, y desde, su puesto.

Por una parte, el empleado debe conocer los riesgos no tecnológicos, por ejemplo:

- información en papel al alcance de personas no autorizadas;
- la falta de confidencialidad de los medios de comunicación tradicionales;
- el peligro de robo o extravío de los dispositivos extraíbles (pendrives, discos duros externos, etc.);
- el acceso físico de terceras personas a las zonas de trabajo (repartidores, personal de limpieza, etc.).

Por otra parte, en muchos puestos de trabajo se tiene acceso a computadores, dispositivos móviles y portátiles con conexión a la red de la empresa y al exterior (internet). Son pues una «puerta de entrada» a la empresa y a sus recursos de información. Para el Grupo Redvoiss, es esencial preparar a los empleados para evitar incidentes que puedan iniciarse en su puesto de trabajo, acentuados por desconocimiento o por falta de preparación:

- accesos no autorizados a los ordenadores y desde ellos a aplicativos de la empresa;
- infecciones por malware;
- robo y fuga de datos en formato digital;
- ataques de ingeniería social, es decir, engaños para manipular a la víctima para obtener información (credenciales, información confidencial, …) o conseguir que realice alguna acción por él (instalar un programa, enviar algunos correos, hacer algún ingreso, etc.).

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en la empresa, debe implantarse una política de protección del puesto de trabajo. En el Grupo Redvoiss, se debe indicar a los empleados las obligaciones y buenas prácticas en materia de seguridad que apliquen a su puesto de trabajo. Esta normativa debe ser firmada por los empleados en su incorporación a la empresa, así como estar siempre disponible y recordar su aplicación de manera periódica.

Objetivos de la protección del puesto de trabajo

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

trabajo.

Controles para aplicar protección del puesto de trabajo

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a protección del puesto de trabajo.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Normativa de protección del puesto de trabajo** Informar al personal sobre la normativa de protección del puesto de trabajo y otra normativa asociada llevando a cabo auditorías periódicas para asegurar su cumplimiento.	☐
A	PRO/TEC	**Destrucción avanzada de documentación mediante mecanismos seguros** Destruir la información confidencial de forma segura teniendo en cuenta el método apropiado para cada soporte de almacenamiento.	☐

NIVEL	ALCANCE	CONTROL	
A	TEC	**Bloqueo programado de sesión** Programar un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo.	☐
B	TEC	**Sistema operativo actualizado** Mantener actualizados los sistemas operativos de los equipos de los usuarios.	☐
B	TEC	**Antivirus actualizado y activo** Mantener el antivirus actualizado y activo en todos los equipos de los usuarios.	☐
B	TEC	**Deshabilitar por defecto los puertos USB** Deshabilitar por defecto los puertos USB y los habilitas para el personal que necesite dicha funcionalidad.	☐
B	TEC	**Seguridad de impresoras y equipos auxiliares** Verificar la seguridad de las impresoras y equipos auxiliares conectados a la red o que puedan almacenar información (Firewalls, contraseñas, …).	☐
A	PER	**Uso de los medios de almacenamiento** Conocer y aplicas las políticas relativas al almacenamiento seguro de la información.	☐
B	PER	**Prohibición de alteración de la configuración del equipo e instalación de aplicaciones no autorizadas** Solicitar al personal informático la instalación de software específico o el cambio de configuración del equipo si es necesario para el desempeño de tu trabajo.	☐
B	PER	**Política de puesto de trabajo limpios** El puesto de trabajo se debe encontrar despejado, sin documentación confidencial ni dispositivos extraíbles al alcance de otras personas.	☐

NIVEL	ALCANCE	CONTROL	
B	PER	**Destrucción básica de documentación mediante mecanismos seguros** Utilizar las destructoras de papel para eliminar la información confidencial.	☐
B	PER	**No abandonar documentación sensible en impresoras o escáneres** Recoger inmediatamente aquellos documentos enviados a imprimir y guardas la información una vez escaneada.	☐
B	PER	**No revelar información a usuarios no debidamente identificados** Conocer la existencia y peligros de la ingeniería social y la información que no se debe desvelar.	☐
B	PER	**Obligación de confidencialidad** Aceptar y cumplir la política de confidencialidad que firmada al incorporarse al puesto de trabajo.	☐
B	PER	**Uso de contraseñas** No publicar ni compartir las claves. Tampoco las anotar en documentos ni en cualquier otro tipo de soporte. Usar contraseñas robustas: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,] , ? , etc.). Cambiar la contraseña periódicamente.	☐
B	PER	**Obligación de bloqueo de sesión y apagado de equipo** Bloquear la sesión al ausentarse del puesto de trabajo y apagar el equipo al finalizar la jornada laboral.	☐
B	PER	**Uso adecuado de Internet** Conocer y aplicar la normativa relativa al uso de Internet.	☐

NIVEL	ALCANCE	CONTROL	
B	PER	**Uso de portátiles y dispositivos móviles propiedad de la empresa** Conocer y aceptar la normativa aplicada al uso de portátiles y dispositivos móviles propiedad de la empresa antes de usarlos como herramienta de trabajo.	☐
A	PER	**Cifrado de la información confidencial** Conocer y aplicar la normativa relativa al cifrado de la información.	☐
B	PER	**Obligación de notificar incidentes** Notificar cualquier incidencia de seguridad (virus, pérdida de información o de dispositivos, etc.).	☐

Controles para aplicar a la protección del puesto de trabajo

- **Normativa de protección del puesto de trabajo.** Se debe contar con una normativa específica que recoja todas las medidas necesarias para proteger el puesto de trabajo, revisando periódicamente su cumplimiento y modificándola si hubiera cambios que la afecten por ejemplo si se cambian los equipos o los sistemas o se adoptan nuevos servicios.

    - También se dará a conocer a los empleados otras políticas relativas a los equipos o servicios que utilicen en su desempeño: correo electrónico, almacenamiento, etc.

- **Destrucción avanzada de documentación mediante mecanismos seguros**. La información obsoleta se destruirá de forma segura según la Política de borrado seguro y gestión de soportes. En particular:

    - mediante destructoras de papel al servicio de los empleados;
    - contratando un servicio externo de destrucción segura, notificando a los empleados de su existencia y obligación de uso;
    - dando a conocer los riesgos asociados a la utilización de papeleras para documentos sensibles (datos personales, información financiera, etc.).

- **Bloqueo programado de sesión.** El personal de TI, programará un bloqueo automático

de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo. Adicionalmente se puede contemplar llevar a cabo la programación del apagado general de equipos una vez terminada la actividad empresarial.

- **Sistema operativo actualizado.** El personal de TI, responsable de los sistemas, aplicará la Política de actualizaciones de software. Revisará los equipos periódicamente para garantizar su actualización o activando las actualizaciones automáticas.

- **Antivirus actualizado y activo.** El personal de TI, es el responsable de los sistemas aplicará la Política antimalware, que incluya la instalación y actualización de herramientas antimalware en todos los equipos y sistemas, y su revisión periódica de manera que se garantice la protección antimalware.

- **Deshabilitar por defecto los puertos USB**. El personal de TI, deshabilitará por defecto los puertos USB de todos los equipos y los habilitará para aquellos usuarios que necesiten, de forma justificada y debidamente autorizada, dicha funcionalidad.

- **Seguridad de impresoras y equipos auxiliares de oficina.** El personal de TI, verificará que las impresoras y otros equipos conectados a la red o que puedan contener información de la empresa están incluidos en las Políticas de seguridad:

    - estarán dentro del perímetro del firewall;
    - se accederá a su panel de configuración mediante contraseña y por canales cifrados;
    - sí se habilita la wifi se ha de configurar su seguridad;
    - sí requiere el uso discos duros, se revisarán las Políticas de almacenamiento
    - sí tienen conectores USB se deshabilitarán;
    - También si fuera posible, se dispondrá de mecanismos de impresión segura (con contraseña) en las impresoras.

- **Uso de los medios de almacenamiento.** Para que el empleado haga un uso correcto de los dispositivos de almacenamiento disponibles, se debe conocer y aplicar la normativa corporativa relativa al almacenamiento local en el equipo de trabajo, almacenamiento en la red corporativa, en la nube y en los dispositivos extraíbles.

- **Prohibición de alteración de la configuración del equipo e instalación de aplicaciones no autorizadas.** Es un riesgo que el empleado cambie la configuración del equipo o instale las aplicaciones que considere necesarias. Esta modificación podría

tener consecuencias de infección de equipos y por lo tanto de pérdida de información. Si el empleado requiere una configuración o software específico para el desempeño de su trabajo, deberá solicitarlo formalmente al equipo informático.

- **Política de puesto de trabajo limpio.** la política de puesto de trabajo limpio, es una obligación el guardar la documentación de trabajo al ausentarse del puesto de trabajo 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. El cumplimiento de esta política conlleva:

    - mantener el puesto de trabajo limpio y ordenado;
    - guardar la documentación y los dispositivos extraíbles que no están siendo usados en ese momento, y especialmente al ausentarnos del puesto o al fin de la jornada laboral;
    - no apuntar usuarios ni contraseñas en post-it o similares.

- **Destrucción básica de documentación mediante mecanismos seguros**. Todo el personal debe utilizar las 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 si los hubiera.

- **No revelar información a usuarios no debidamente identificados.** La información es uno de los activos empresariales más cotizados. Por este motivo es posible que alguien intente obtener parte de esta información (contraseñas de usuario, información de cuentas bancarias, 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: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,], ?, etc.);
    - se deben cambiar periódicamente.

- **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 entornos 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 (ambas expresadas en este documento) que indica qué 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 tabletas) y dispositivos externos de almacenamiento (USB, CD/DVD, etc.);
    - borrado accidental de 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.

Gestión de dispositivos móviles no corporativos (BYOD)

En el Grupo Redvoiss, se permite el uso controlado de dispositivos personales (portátiles, smartphones, tablets), propiedad del empleado, en el ámbito corporativo es lo que se conoce como BYOD (Bring Your Own Device). Se trata de una práctica muy frecuente, por lo tanto, se debe prestar una especial atención para que su uso no comprometa la seguridad de la información de la empresa. Tomando esto en consideración, se tiene presente ciertos riesgos que se debe conocer antes de permitir el uso de dispositivos personales en el ámbito corporativo:

- La exposición a redes inseguras en el ámbito personal. Este tipo de conexión podría tener como consecuencia que la información corporativa fuera accesible o pudiera ser interceptada por terceras personas no autorizadas.

- La instalación de aplicaciones que solicitan permisos para acceder a partes del dispositivo donde puede haberse almacenado información sensible, e incluso solicitar la activación de la geolocalización.

- La inexistencia de mecanismos de control de acceso a los dispositivos y la ausencia de

medidas de seguridad en cuanto al almacenamiento de la información. Si alguien tuviera acceso a nuestro dispositivo no tendría ninguna dificultad a la hora de acceder o extraer información confidencial.

- La carencia de herramientas antivirus y de una normativa de actualizaciones adecuada. Actualizar las aplicaciones y disponer de un antivirus protegen al terminal de posibles ataques y accesos no autorizados.

- La opción (activada) de recordar y usar contraseñas de forma automatizada para acceder a redes, aplicaciones, sitios web, etc. Si alguien tuviera acceso al dispositivo no necesitaría disponer de las credenciales de usuario para acceder a la información.

Una vez establecida la política de seguridad relativa al uso seguro de los dispositivos personales para el trabajo, debe ponerse en conocimiento de los empleados y ser aceptada por los mismos antes de que utilicen sus dispositivos para acceder a aplicaciones o tratar con información de la empresa.

Objetivos de la gestión de dispositivos móviles no corporativos (BYOD)

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

Controles para aplicar en la gestión de dispositivos móviles no corporativos (BYOD)

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al uso de dispositivos móviles no corporativos (BYOD).

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Normas y procedimientos BYOD** Elaborar normas y procedimientos específicos si permites BYOD en la empresa (usos permitidos, antivirus, actualización, configuraciones, …)	☐
B	PRO	**Prohibición de uso de dispositivos manipulados** Prohibir el uso de dispositivos *rooteados* o a los que se ha realizado *jailbreak*.	☐
B	PRO	**Concienciación de los empleados** Involucrar a los usuarios en la protección de sus propios dispositivos y de los datos que contienen o a los que pueden acceder.	☐
B	PRO	**Formación de los empleados** Proporcionar a los empleados, charlas o formación sobre cómo proteger sus dispositivos (contraseñas, actualizaciones, permisos, etc.).	☐
B	PRO	**Limitar el acceso a redes externas** Prohibir el uso de redes inalámbricas externas no corporativas salvo 3G/4G.	☐
B	PRO/TEC	**Lista de aplicaciones no permitidas** Mantener una lista de aplicaciones no permitidas y la difundes entre tus empleados.	☐
B	PRO/TEC	**Controlar el almacenamiento en la nube de datos corporativos** Supervisar el uso de aplicaciones de almacenamiento en la nube.	☐

NIVEL	ALCANCE	CONTROL	
B	PRO/TEC	**Proceso de borrado de la información** Aplicar una normativa de entrega/eliminación de la información de sus dispositivos cuando el empleado abandona la empresa.	☐
A	TEC	**Control de acceso a la red** Implementar un control de acceso (autenticación con contraseñas, doble factor, VPN…) a la red corporativa desde estos dispositivos.	☐
B	TEC	**Control de usuarios y dispositivos** Mantener un registro actualizado con usuarios, dispositivos y privilegios de acceso.	☐
B	TEC	**Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos** Instalar y configurar medidas para el almacenamiento seguro a la información (clasificación de información, cifrado de datos, etc.)	☐
B	TEC/PER	**Bloqueo programado** Configurar el bloqueo automático del dispositivo tras un periodo de inactividad.	☐
A	TEC/PER	**Extravío de dispositivos** Configurar medidas de seguridad para proteger la información corporativa en los dispositivos (localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas) en caso de extravío.	☐
B	PER	**Desconexión wifi y Bluethooth** Desactivar en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no son necesarios.	☐
B	PER	**Cumplimiento de la normativa** Conocer y aceptar la normativa corporativa vigente para el uso de tus dispositivos en actividades de la empresa.	☐

Controles necesarios para en la gestión de dispositivos móviles no corporativos (BYOD)

- **Normas y procedimientos BYOD**. Se debe elaborar normas y procedimientos específicos que regulen el uso de dispositivos BYOD (listado de dispositivos autorizados, en qué condiciones se permite su uso, cómo se accede a la información, configuraciones de seguridad necesarias para poder utilizarlos, etc.).

- **Prohibición de uso de dispositivos manipulados**. Se recomienda prohibir el uso de dispositivos rooteados o a los que se les ha hecho jailbreak ya que permiten la instalación de aplicaciones de repositorios no oficiales.

- **Concienciación de los empleados.** Los dispositivos como el teléfono móvil o el portátil son susceptibles de robo. Por ello es importante involucrar a los usuarios en la protección de sus propios dispositivos concienciándolos de la trascendencia de la protección del mismo y de los datos que contiene.

- **Formación de los empleados.** Proporcionaremos a los empleados formación suficiente para un uso seguro de los dispositivos. Por ejemplo, han de saber:

    - configurar los parámetros de seguridad de los dispositivos;
    - actualizar tanto el sistema operativo como las aplicaciones periódicamente (en especial el antivirus);
    - no instalar aplicaciones que exijan permisos que pongan en riesgo la información confidencial (acceso a la agenda, geolocalización, etc.);
    - bloquear los dispositivos con contraseña y activar el bloqueo automático tras un periodo corto de inactividad;
    - no desatender los dispositivos al viajar en transporte público.

- **Limitar el acceso a redes desconocidas**. Los usuarios deben conocer que es preferible optar por la conexión de datos de su móvil 3G/4G/... cuando las redes inalámbricas disponibles sean desconocidas. Estas redes wifi deben considerarse inseguras.

- **Lista de aplicaciones no recomendadas.** Estableceremos una lista de tipos de aplicaciones que no se podrán instalar en estos dispositivos por el peligro que suponen para la información corporativa. Estas aplicaciones pueden requerir para su instalación acceso a datos confidenciales de la organización (datos de la agenda, geolocalización del terminal, etc.).

- **Controlar el almacenamiento de datos corporativos.** Las aplicaciones personales en los dispositivos móviles para el tratamiento de datos en la nube no son tan seguras como las empresariales por lo que hay que prestar especial atención a este intercambio de archivos. Se puede permitir la consulta de información en la nube, pero se recomienda no actualizarla desde estos dispositivos personales.

- **Proceso de borrado de la información.** Se debe establecer el proceso a seguir para entregar/eliminar la información en estos dispositivos cuando el empleado abandona la empresa.

- **Control de acceso a la red.** El acceso a la red corporativa a través de dispositivos personales debe estar integrado en el sistema de control de accesos (autenticación, doble factor, …). De esta forma el empleado debe acreditar su identidad antes de acceder a los servicios de la red corporativa. Para mayor seguridad la empresa puede proporcionar a sus empleados acceso mediante red privada virtual (VPN) que cifra las comunicaciones.

- **Control de usuarios y dispositivos.** Mantendremos un registro de usuarios y dispositivos que tienen 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.

- **Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos.** Por ejemplo:

    - Implementaremos en los dispositivos mecanismos de cifrado de la documentación además de los de autenticación de usuarios.
    - Impediremos guardar de forma automática las credenciales de usuarios asociadas a las herramientas corporativas.

- **Bloqueo programado.** Configuraremos el dispositivo para que se bloquee automáticamente tras un periodo de inactividad.

- **Extravío de dispositivos.** Ante la posibilidad de pérdida o extravío de este tipo de dispositivos, estableceremos las siguientes medidas:

    - Localización mediante GPS, wifi o la información de la antena de telefonía con la que esté conectado el dispositivo. Una vez marcado como «perdido», el Smartphone empieza a enviar los datos de su ubicación de manera constante a

una cuenta previamente configurada (correo, SMS, central de control...).
  - Tener siempre activado el bloqueo de pantalla del terminal. En caso contrario se bloqueará de manera remota.
  - Borrado remoto de datos: esta opción permite que los datos contenidos en el dispositivo se borren de manera remota, impidiendo su utilización por un usuario no legítimo.
  - Vigilar las aplicaciones que se ejecutan. El seguimiento de las llamadas
  - efectuadas y las redes sociales accedidas entre otros, suelen ser datos suficientes para obtener nombres, apellidos y hasta direcciones de un posible delincuente.

- **Desconexión wifi y Bluethooth.** Se desactivará en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no sean necesarios.

Uso de técnicas criptográficas

La información sensible y confidencial que manejamos en la empresa:

- bases de datos, registros de usuarios, correos electrónicos confidenciales;
- información sujeta a protección legal;
- backups;
- información confidencial en dispositivos extraíbles y móviles;
- credenciales de acceso y para pagos online, etc.

por su trascendencia para nuestro negocio debe estar especialmente protegida tanto en tránsito como cuando está almacenada. Para proteger esta información, además de controlar el acceso a la misma y proteger los sistemas con los que la manejamos, se deben aplicar herramientas criptográficas que cifren nuestros datos, haciéndolos ilegibles por aquellos que no dispongan de la clave de cifrado. De esta manera garantizaremos la confidencialidad e integridad de la información sensible cuando está almacenada.

Las técnicas criptográficas permiten también firmar digitalmente documentos y correos electrónicos relevantes (como facturas, contratos, etc.), lo que garantiza además la autenticidad y no repudio de los mismos. Esto es muy útil en el caso de realizar ciertas gestiones online, como las realizadas con la administración.

Tanto para el cifrado de la información como para el uso de la firma digital, se deberá realizar un análisis previo que determine claramente que datos de la empresa se deben cifrar y que situaciones o usuarios requieren de firma digital. Asimismo, cabe destacar la importancia de

utilizar protocolos seguros en nuestras comunicaciones, tanto para nuestros empleados como para los usuarios de nuestros servicios. En particular se aconseja el uso de los certificados web de validación extendida para los servicios gestionados a través de la web (sobre todo si conllevan transacciones económicas como en las tiendas online y conexión con la extranet de clientes corporativos) o el uso de VPN para el acceso de teletrabajadores.

Controles para aplicar la gestión del uso de técnicas criptográficas

Garantizar que se hace un uso adecuado y eficaz de las técnicas criptográficas para asegurar la confidencialidad, integridad, autenticidad y el no repudio de la información sensible manejada por la empresa, tanto almacenada como en tránsito. Por ejemplo: datos de carácter personal, información sensible o información confidencial, backups en la nube o en proveedores externos, datos en móviles o dispositivos extraíbles, contratos, facturas e intercambios comerciales o con las Administraciones Públicas, accesos remotos, etc.

Controles para aplicar la gestión del uso de técnicas criptográficas

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a almacenamiento en la red corporativa.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** Aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** Aplica al personal técnico especializado.
- **Personas (PER):** Aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Información susceptible de ser cifrada** Identificar qué información de la empresa debería ser cifrada.	☐
B	PRO/TEC	**Uso de firma electrónica** De ser factible, implantar el uso de la firma electrónica en los servicios extranet con clientes y con la Administración de servicios web.	☐
B	PRO/TEC	**Certificados web** Adquirir certificados web el sitio web comparativo.	☐
B	PRO/TEC	**Cifrado de datos sensibles cuando se contratan servicios externos** Comprobar que se utilizan canales cifrados para las comunicaciones y herramientas de cifrado en el tratamiento de la información sensible al contratar servicios.	☐
B	PRO/TEC	**Cifrado de datos sensibles cuando se solicitan desarrollos de aplicaciones** Comprobar que se cifran las credenciales de acceso cuando se solicitan desarrollos web o de apps que impliquen *login* de usuarios.	☐
B	PRO/TEC	**Acceso desde el exterior con VPN** Autorizar el acceso desde el exterior al personal que lo necesite estableciendo canales VPN cifrados.	☐
B	TEC	**Algoritmos de cifrado autorizados** Aplicar y revisar los algoritmos de cifrado más adecuados para los sistemas de cifrados internos (por ejemplo, Backups y archivos zip compartidos por correo).	☐
B	TEC	**Aplicaciones autorizadas para usos criptográficos** Disponer de una lista de aplicaciones autorizadas para cifrado.	☐
B	TEC	**Uso de protocolos seguros de comunicación** Implementar protocolos seguros para acceder (administración, transferencia de ficheros, …) a los servidores tanto si están en nuestras instalaciones como si están en algún proveedor.	☐

NIVEL	ALCANCE	CONTROL	
B	TEC	**Cifrado de la wifi de la empresa** Configurar la wifi de la empresa con el estándar de cifrado más seguro, actualmente WPA2.	☐

Controles necesarios para la gestión del uso de técnicas criptográficas

- **Información susceptible de ser cifrada.** La clasificación de la información permite saber qué información debe ser cifrada para garantizar su confidencialidad e integridad. Dicha información puede ser:

  - información sensible, de carácter personal o confidencial;
  - registros con credenciales de autenticación;
  - información almacenada en dispositivos personales o de terceros (incluidos los servicios cloud) que carecen de los controles de seguridad adecuados;
  - información transferida a través de redes de telecomunicación no confiables o en soportes de almacenamiento físicos no protegidos adecuadamente.

- **Uso de firma electrónica.** La implementación de la firma electrónica, permite en aquellos escenarios en los que sea imprescindible, el garantizar la autenticidad y el no repudio de la información, como para realizar trámites con las Administraciones Públicas o emitir facturas. En este caso, se tiene que elegir qué tipo de certificado de representación legal que se requiere implantar:

  - certificado de persona jurídica;
  - certificado de pertenencia a empresa;
  - certificado de representante;
  - certificado de factura electrónica.

  Seleccionaremos el prestador de servicios que generará nuestros certificados. Además, se debe controlar:

  - periodo de validez;
  - posibilidad de revocación;
  - cumplimiento con la legislación (prestadores cualificados);
  - gestión de su almacenamiento.

- **Certificados web**. Se requieren para garantizar la seguridad de la información en nuestro sitio web, este debe ser un certificado web (SSL/TLS):

    - para un dominio, múltiples dominios y subdominios;
    - validación de dominio, de la organización y validación extendida.

- **Cifrado de datos sensibles cuando se contratan servicios externos**. Si se necesita contratar servicios externos que traten datos confidenciales o sensibles verificaremos que las trasferencias de datos son seguras, bien cifrando los datos antes de transferirlos o bien utilizando canales seguros. Estos son algunos ejemplos:

    - Para contratar un servicio de gestión que incluya el tratamiento de datos personales (por ejemplo: nóminas, seguridad social, …) o confidenciales, se debe asegurar que las transferencias de datos se realizan con canales cifrados (por ejemplo, vía VPN o cifrando los datos antes de enviarlos);
    - Al realizar backups en la nube de archivos que contengan datos confidenciales o datos personales de empleados o clientes, deben ser cifrados;
    - En el caso de contratar pasarelas de pago para algún servicio online al cliente, siempre que sea posible, es preferible no almacenar datos de transacciones en nuestra web (cuentas, tarjetas,…), eligiendo proveedores que hagan toda la transacción cumpliendo el estándar PCI-DSS.

- **Cifrado de datos sensibles cuando se solicitan desarrollos de aplicaciones.** Al momento de contratar el desarrollo de un aplicativo web o una app para dispositivos móviles que ofrezca acceso a nuestros usuarios (login), las claves de acceso han de almacenarse cifradas. Todos los desarrollos que traten datos personales deben contemplar criterios de privacidad por defecto y por diseño.

    - La privacidad por diseño es la que incorpora, desde que se concibe un servicio hasta en su despliegue y operación, las medidas tecnológicas para preservar la privacidad de los usuarios.
    - La privacidad por defecto protege los datos del usuario en los ajustes por defecto. El diseñador de los servicios, bien por su construcción, o en los parámetros configurables por el usuario, elegirá los más respetuosos con la privacidad, no permitiendo funcionalidades extendidas por defecto que afecten a los datos de los usuarios, a no ser que este las elija explícitamente.

- **Acceso desde el exterior con VPN.** Se Requiere de forma obligatoria para las

conexiones de trabajo remoto, solo se debe autorizar el acceso desde el exterior a los servidores de nuestras instalaciones por los canales habilitados de VPN por medios cifrados que garanticen la confidencialidad e integridad de las comunicaciones siguiendo la Política de uso de wifis y conexiones externas.

- **Algoritmos de cifrado autorizados.** Para evitar el uso de sistemas de cifrado obsoletos, se debe aplicar algoritmos de cifrado actuales comprobando que estén vigentes. Se tendrán en cuenta de forma prioritaria los algoritmos y sistemas de cifrado de carácter abierto y de especificación pública (conocidos y evaluados ampliamente). Se debe hacer uso de sistemas de cifrado asimétrico en detrimento de los sistemas de cifrado simétrico.

- **Aplicaciones autorizadas para usos criptográficos.** Se debe tener una lista de las aplicaciones autorizadas para fines criptográficos. Asimismo, detallar el uso concreto de cada una de ellas en cada caso que se vaya implementado, como las siguientes:

    - cifrado del disco de arranque;
    - cifrado de discos internos y extraíbles;
    - cifrado de correo;
    - cifrado de backups;
    - cifrado de ficheros y directorios;
    - cifrado de dispositivos móviles.

- **Uso de protocolos seguros de comunicación.** Se debe proporcionar a los empleados, si las necesitan para su actividad, formación y herramientas de comunicación que utilicen protocolos criptográficos actualizados. De esta forma se debe de garantizar la confidencialidad al acceder a nuestros sistemas, tanto si se ubican en nuestras instalaciones o como si se ubican en las instalaciones de proveedores. Entre otros se incluyen los siguientes protocolos:

    - SSH para el acceso seguro remoto a la administración de equipos (no utilizar Telnet que no va cifrado);
    - SFTP/FTPS para la transferencia segura de ficheros;
    - HTTPS para la transferencia segura de datos en servicios web críticos (pagos online, conexión extranet con clientes, descarga de información sensible, etc.).

- **Cifrado de la wifi de la empresa.** Configurar la wifi de la empresa con el estándar de cifrado más seguro, actualmente WPA2, importante el cambiar la clave de acceso por defecto.

Gestión de acceso desde redes externas por VPN y WIFI

Es habitual tener que acceder a los datos de la empresa cuando estamos fuera del lugar de trabajo (viajes, reuniones, teletrabajo, etc.). En ocasiones no podemos hacer uso de las redes o conexiones 4G/5G, lo que nos obliga a conectarnos a redes domésticas o a redes públicas (hoteles, cafeterías, aeropuertos, etc.) que en la mayoría de los casos podrían no ser seguras.

Es prudente asumir que, por defecto, las redes inalámbricas que utilizan los trabajadores fuera del entorno de la red del Grupo Redvoiss, no disponen de las medidas de seguridad necesarias para la protección de los datos y las comunicaciones corporativas. A menudo, la información confidencial de nuestra empresa se transmite a través de redes inalámbricas cuya seguridad no está bajo nuestro control, por lo que debemos asegurarnos de que los datos viajan convenientemente protegidos antes de hacer uso de estas redes.

El Grupo Redvoiss, establece las condiciones y circunstancias en las que se permite el acceso remoto a sus servicios corporativos. Es decir, se determina y controla, quién puede acceder a qué, cómo y cuándo. Esta tarea implica disponer de los medios necesarios para llevarla a cabo y ofrecer la correspondiente formación a los trabajadores para que conozcan cómo conectarse de forma segura y cómo mantener sus equipos seguros cuando viajan o se conectan desde el exterior.

Una de las herramientas de seguridad que implementamos para permitir el acceso remoto corporativo desde el exterior del Grupo Redvoiss, es la utilización de una Red Privada Virtual o VPN (en este caso implementando las fortalezas de seguridad de nuestro firewall con su agente **VPN**). Se debe usar la VPN cuando se necesita acceder a información confidencial de manera remota, y la red que estemos utilizando no ofrezca las suficientes garantías de seguridad. Estas son las ventajas de utilizar una VPN:

- toda la información se transmite de manera segura gracias al cifrado de datos y de conexión;
- confidencialidad e integridad de la información: debe ser cifrada, la información no puede ser leída, modificada o alterada durante la transmisión;
- la información solo se trasmite entre dispositivos autorizados y configurados para este fin;
- restricción de acceso: a través de usuario y contraseña necesitando una previa autorización;
- fácil ampliación del número de usuarios.

Las conexiones establecidas utilizando VPN protegen la información que se intercambia, ya que establecen un canal cifrado de comunicación entre nuestro dispositivo y nuestro lugar de trabajo por donde «viajan» nuestros datos de manera segura.

Objetivos de la gestión de acceso desde redes externas por VPN y WIFI

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.

Controles para aplicar la gestión de acceso desde redes externas por VPN y WIFI

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a almacenamiento en la red corporativa.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** Aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** Aplica al personal técnico especializado.
- **Personas (PER):** Aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO/TEC	**Política de conexión** Elaborar una normativa corporativa para regular las conexiones externas.	☐

NIVEL	ALCANCE	CONTROL	
A	TEC	**Configuración de la VPN** Configurar solo conexión VPN para acceder desde el exterior. Crear cuentas de usuario con permisos de acceso. Detallar el software permitido para realizar estas conexiones. Establecer un tiempo de desconexión automática de la VPN tras un periodo de inactividad.	☐
B	PER	**Uso de la VPN** Conocer cómo conectarte vía VPN (si la empresa lo permite) y en qué situaciones se debe hacer.	☐
B	PER	**Acceso a redes wifi externas** Al conectar a una nueva red inalámbrica, comprobar que utiliza el protocolo WPA2. Comprobar que los sitios a los que se accede tienen certificado y utilizan protocolos seguros (https://) si se va a realizar actividades críticas.	☐
A	PER	**Configuración de la wifi doméstica** Antes de utilizarlas, configurar el protocolo WPA2, y cambiar el nombre del SSID y las credenciales por defecto.	☐
B	PER	**Redes inalámbricas de los dispositivos móviles** Abrir las conexiones wifi y *bluetooth* de los dispositivos móviles solo cuando se van a utilizar y para conectarte a dispositivos confiables.	☐
B	PER	**Uso de dispositivos móviles** Revisar las políticas de uso de dispositivos móviles y uso de dispositivos personales en el ámbito corporativo.	☐
B	PER	**Uso de ordenadores no corporativos** Evitar el uso de dispositivos no corporativos. Revisar la seguridad de tus dispositivos domésticos y tomar precauciones cuando utilices dispositivos de uso compartido.	☐

Controles necesarios para la gestión de acceso desde redes externas por VPN y WIFI

- **Política de conexión.** La dirección debe determinar si la política de seguridad permite la conexión desde redes externas a los recursos de la empresa y establecer las condiciones este tipo de accesos.

- **Configuración de la VPN.** Para los accesos permitidos desde el exterior el equipo técnico de TI, debe disponer y configurar un servicio VPN:

    - crear cuentas de usuario con permisos de acceso personalizados;
    - determinar el software permitido para realizar conexiones VPN;
    - establecer un tiempo para la desconexión automática de la VPN tras un periodo de inactividad;

- **Uso de la VPN.** Los empleados que tengan autorizado el acceso vía VPN, deben conocer cómo hacerlo y cuándo está permitido:
    - Solo cuando se utilice redes públicas o no confiables;
    - para acceder a los recursos corporativos como impresoras, documentos, servidores de base de datos, aplicaciones específicas, etc.;
    - cuando se necesite hacer operaciones confidenciales: acceso a bases de datos, conexión con clientes, banca online o facturación, que impliquen la transmisión de usuarios, contraseñas, o cualquier otra información confidencial;
    - cuando se requiere interconectar redes separadas de forma segura: distintos edificios u oficinas separadas geográficamente, equipos utilizados en teletrabajo con la oficina, etc.;
    - cuando se requiera el uso para el teletrabajo.

- **Acceso a redes wifi externas.** Al conectarte a una red inalámbrica desconocida, compruebas que utiliza el protocolo WPA2 y revisas el uso vas a hacer de esa red:

    - Sólo utilizar redes wifi púbicas no seguras para realizar actividades de bajo riesgo como navegar o leer noticias, pero asegúrate que el canal está cifrado (sitio web con https:// y certificado) si se va iniciar sesión (hacer login) o suscribirte.

    - Sólo utilizar redes wifi públicas seguras (al menos con WPA2) si no tienes otro medio más seguro (redes móviles 4G/5G o una VPN) a tu alcance para realizar actividades de alto riesgo (uso de email, trabajar con documentos online, redes sociales, banca online o compras online) comprobando además que acceder a

sitos webs legítimos, cifrados (https://) y con certificado.

- **Configuración de la wifi doméstica.** En el caso de usar una wifi doméstica, se tiene que configurarla para:

    - activar el protocolo WPA2;
    - cambiar el nombre por defecto del SSID;
    - cambiar las credenciales por defecto;

- **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.** Al utilizar dispositivos móviles para trabajar fuera de la empresa, se han de tomar las medidas de seguridad indicadas en la de uso de dispositivos móviles no corporativos.

- **Uso de dispositivos no corporativos**. Si utilizas dispositivos de uso público evita realizar actividades de alto riesgo (uso de email corporativo, trabajar con documentos online, redes sociales, banca online o compras online). Desconfía de la seguridad del equipo y sus conexiones. En cualquier caso, si se tiene la necesidad de utilizarlos para hacer login en algún servicio corporativo siempre que esté permitido y no puedas hacer uso de una VPN:

    - revisar el entorno para evitar la mirada de observadores o de cámaras
    - utilizar el modo de navegación privada del navegador;
    - teclear la URL o dirección web, en lugar de utilizar el buscador;
    - verificar que la página a la que accedes es auténtica, que utiliza protocolo https:// y que tiene certificado y está vigente;
    - evitar que el navegador guarde las contraseñas;
    - al finalizar la sesión borrar el historial de navegación y las cookies en el navegador;
    - no conectar pendrives ni otros dispositivos externos;
    - revisar que no dejar ningún archivo personal en el equipo.

    Si utilizas dispositivos domésticos:

    - actualizar el software de sistemas operativos y aplicaciones;
    - utilizar un usuario no compartido;

- instalar y activar un antivirus y el firewall del sistema operativo;
- no instalar aplicaciones sin licencia o cuyo origen desconozcas.

Gestión de protección de antivirus y antimalware

La aparición constante de nuevos virus y otros tipos de malware, es una de las principales amenazas a las que se enfrentan hoy en día nuestros sistemas. Las vías de contagio por malware son numerosas, destacando entre otras:

- las descargas de ficheros de todo tipo, adjuntos en correos o desde páginas web;
- la navegación por webs de dudosa fiabilidad;
- y la utilización de dispositivos ajenos, por ejemplo, pendrives.

El enorme daño que pueden causar a nuestra organización hace obligatorio el establecimiento de una política de control de malware. En el Grupo Redvoiss, implementamos la solución de **Antivirus de Deep Instinct**. De este modo, podemos prevenir, detectar, controlar y eliminar la ejecución de cualquier software malicioso en nuestros sistemas.

Objetivos de la gestión de protección de antivirus y antimalware

Proteger todos los activos de información de la empresa contra la infección por virus o cualquier otro tipo de malware.

Controles para aplicar la gestión de protección de antivirus y antimalware

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a almacenamiento en la red corporativa.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** Aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** Aplica al personal técnico especializado.
- **Personas (PER):** Aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Instalar y desplegar la solución antimalware** implementar y mantener los dispositivos actualizados.	☐
A	TEC	**Configurar las herramientas de detección de malware** Configurar correctamente todas las funcionalidades de las herramientas de control de malware.	☐
B	TEC	**Actualizar las herramientas de detección de malware** Actualizas cada de forma automática las herramientas de detección y control de malware que se tienen instaladas.	☐
A	TEC	**Establecer el procedimiento de respuesta ante la infección por ejecución de malware** Elaborar procedimientos detallados de actuación ante infecciones por malware.	☐
B	PER	**Buenas prácticas para el control de malware** Seguir las directrices básicas para prevenir las infecciones por malware.	☐

Controles necesarios para la gestión de protección de antivirus y antimalware

Determinar qué tipo de soluciones serán las más convenientes para nuestra empresa. Dependiendo del tamaño de nuestra organización, del nivel de seguridad necesario y de la complejidad de las configuraciones para la protección de nuestros activos de información, podremos determinar distintos tipos de soluciones:

- herramientas para el puesto de trabajo, el portátil o los dispositivos móviles, soluciones globales corporativas entre ellas:

    - UTM o gestión unificada de amenazas;
    - servicios gestionados que nos pueden facilitar nuestros proveedores de servicios

de internet (ISP) u otros proveedores desde un centro de operaciones de seguridad o SOC;
- soluciones de seguridad ofrecidas como servicios en la nube que monitorizan nuestros equipos de forma remota.

En el Grupo Redvoiss, implementamos la solución de **Antivirus de Deep Instinct,** la cual se elogió por la compatibilidad con nuestra infraestructura y la versatilidad (antimalware, antiphishing, antispam, análisis de web y correo, …) que posee la herramienta.

- **Configurar las herramientas de detección de malware.** Para un uso eficiente de las herramientas de control de malware se debe realizar una correcta configuración de todas sus funcionalidades. La configuración deberá permitirnos, entre otros, establecer los siguientes controles:

  - realizar análisis automáticos y periódicos para detectar malware;
  - realizar comprobaciones automáticas de los ficheros adjuntos al correo y de las descargas web, ya que pueden contener código malicioso ejecutable;
  - bloquear el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas negras;
  - permitir el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas blancas;
  - permitir el análisis de páginas web para detectar posibles amenazas incluidas en las mismas.

- **Actualizar las herramientas de detección de malware**. Se debe determinar la periodicidad con la que las herramientas de detección de malware son actualizadas. Actualmente se crean miles de virus al día, por lo que las actualizaciones de la base de datos de firmas de virus deberían ser automáticas y tener una periodicidad como mínimo diaria. Por otro lado, y como cualquier otra aplicación crítica, se debe actualizar convenientemente el propio software antivirus.

- **Establecer el procedimiento de respuesta ante la infección por ejecución de malware.** En primer lugar, determinar qué sucesos serán considerados como incidencias por ejecución de malware, analizando:

  - el impacto del ataque y los activos que puedan estar comprometidos;
  - la forma de recuperar los activos impactados;
  - los canales adecuados de aviso y notificación.

- Después estableceremos las responsabilidades y la operativa a seguir en cada caso:

    - desinfección y eliminación de ficheros;
    - aviso a soporte técnico del fabricante;
    - reinstalación de software afectado;
    - desconexión y asilamiento del equipo afectado y el registro formal del incidente.

- **Política general de buenas prácticas para el control de malware**. Con el fin de reforzar las medidas establecidas para el control del malware es conveniente tener concienciada a la plantilla en los siguientes aspectos:

    - Se deben considerar todos los contenidos y las descargas como potencialmente inseguros hasta que no sean convenientemente analizados por una herramienta de detección de malware.
    - Deben prohibirse las siguientes acciones:

        - Ejecutar ficheros descargados de servidores externos, de soportes móviles no controlados o adjuntos a correos, sin haber sido previamente analizados.
        - Configurar el programa cliente de correo electrónico para la ejecución automática de contenido recibido por correo.
        - Alterar la configuración de seguridad establecida para los sistemas y equipos de tratamiento de información.

    - Debe utilizarse únicamente el software permitido por la organización. Este además debe estar convenientemente actualizado.
    - Para evitar la recepción de spam se deben seguir las directrices incluidas en la política de correo electrónico.