

1. Objetivo

Establecer los lineamientos y políticas generales de Seguridad de la Información para todos los colaboradores de Concrearmado Ltda.

2. Alcance

Aplican para todos los procesos y colaboradores responsables de su ejecución que hacen parte de CONCREARMADO LTDA y las sociedades bajo la administración de Concrearmado Ltda.

3. Políticas y lineamientos

3.1 Uso de medios de almacenamiento extraíbles o removibles

Generalidades

La utilización de dispositivos removibles o extraíbles de almacenamiento (Memorias USB/Flash, SD, microSD, CD/DVD re escribibles, discos duros portátiles, dispositivos electrónicos como celulares, tabletas, entre otros) por parte de los usuarios, se encuentra restringido y monitoreado, y podrá ser autorizado a algunos empleados o colaboradores de CONCREARMADO LTDA que lo requieran, cumpliendo con los lineamientos estrictamente establecidos por la empresa. El colaborador que los utilice con la autorización respectiva deberá buscar en todo momento preservar la Confidencialidad de la información de la empresa almacenada en éste, así como evitar contagiar la red de la empresa de código malicioso o dañino (virus, troyanos, Spyware, etc.).

Justificación

Por esta razón CONCREARMADO LTDA. reconoce la necesidad de definir una política para asegurarse de que la información propietaria, adquirida o puesta en custodia en la empresa no está supeditada a fuga, uso no autorizado, modificación, divulgación o pérdida y que esta debe ser protegida adecuadamente según su valor, confidencialidad e importancia. Así mismo, el proceso de TI, con el propósito de dar cumplimiento a los objetivos del Sistema de Seguridad de la Información y los de la empresa, determinan la presente Política que define el manejo y limitaciones de este tipo de dispositivos.

El uso de dispositivos de almacenamiento externo está permitido en CONCREARMADO LTDA, para los funcionarios, contratistas y demás colaboradores; con el fin de facilitar el compartir y transportar **información que no sea de carácter confidencial ni sensible** de la empresa dentro de las normas y responsabilidades del manejo de información institucional.

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos, mediante una conexión inalámbrica directa a cualquier equipo de cómputo de la empresa. Entre estos, se pueden encontrar, pero no se limitan a:

- Memorias Flash USB
- Reproductores portátiles MP3/MP4
- Cámaras con conexión USB
- iPhones / Smartphones
- SD Cards/ Mini SD Cards/ Micro SD Cards.
- PDAS / Tablets
- Dispositivos con tecnología Bluetooth.
- Tarjetas Compact Flash

- Discos duros de uso externo
- Cámaras fotográficas y/o video

Constituye un uso indebido de dispositivos de almacenamiento externo:

- Almacenar o transportar información sensible, confidencial o reservada de la empresa.
- Ejecutar cualquier tipo de programa no autorizado por la empresa desde cualquiera de las unidades de almacenamiento en mención.
- Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del usuario de alguno de estos medios de almacenamiento.
- Usar dispositivos de almacenamiento externo en actividades que resulten violatorias del ordenamiento jurídico colombiano vigente.
- Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información privada de los usuarios o colaboradores de la empresa. En concordancia con lo anterior, queda restringido el uso de Dispositivos de Almacenamiento Externo, en todas las áreas de la empresa

Obligaciones de los colaboradores:

- Uso de medios de almacenamiento extraíbles autorizados
- Evitar hacer copias de respaldo de información en estos medios, se debe guardar en los repositorios de la compañía para el almacenamiento de información, según corresponda.
- No divulgar, ni transferir la información almacenada en los medios extraíbles a personas ajenas a la empresa. Esto puede comprometer la confidencialidad de la información de CONCREARMADO LTDA.
- Los usuarios o personas que pertenezcan a servicios tercerizados contratados por la empresa, no podrán utilizar dispositivos removibles o extraíbles de almacenamiento (Memorias USB/Flash, SD, microSD, CD/DVD re escribibles, discos duros portátiles, dispositivos electrónicos como celulares, tabletas, entre otros) diferentes a los asignados y autorizados para cumplir o ejecutar sus labores en las instalaciones teniendo en cuenta situaciones en las cuales posea o manipule información de la empresa.

En caso de utilizar los medios de almacenamiento extraíbles autorizados en un equipo de cómputo diferente al de la empresa, se deben tener en cuenta las siguientes recomendaciones:

- Al momento de conectar los medios de almacenamiento extraíbles al equipo de cómputo de la empresa, realiza un escaneo previo con el antivirus autorizado por la empresa, con el fin de evitar que se transfieran virus informáticos y software malicioso.
- Previo a copiar información almacenada de los medios de almacenamiento extraíbles a los discos locales del equipo de cómputo asignado se debe realizar un escaneo con el antivirus dispuesto por la empresa.
- No exponer los medios de almacenamiento extraíbles en lugares públicos.
- Proteger los medios de almacenamiento extraíbles de humedad y golpes.
- Evitar consumir bebidas durante la utilización de los medios extraíbles.

3.2 Uso repositorios de la compañía

Descripción

CONCREARMADO LTDA ofrece 3 tipos de repositorios institucionales, con el propósito de garantizar, respaldar, asegurar, proteger y centralizar la información de cada proceso. El acceso a los repositorios institucionales se da a través del usuario y contraseña asignados a los colaboradores para la sesión de red o cuenta de correo electrónico y de los permisos establecidos en el servidor para el almacenamiento de la información de cada proceso; por lo cual el manejo de los repositorios es responsabilidad exclusiva de los colaboradores.

Justificación

El acceso y empleo de servicios de almacenamiento de archivos On Line, es decir, aquellas unidades virtuales de almacenamiento personal por medio de internet, en las cuales se incluye, pero no se limitan los servicios de Google Drive, Skydrive, Dropbox, Rapidshare, GigaSize, MediaFire, 4shared, etc; **están prohibidos**. Las únicas herramientas permitidas son:

- Onedrive Empresarial
- Sharepoint Online(asignado por la empresa)
- Synology(Almacenamiento interno de la empresa)

El área de Tecnologías de la Información y Comunicación, garantizará la disponibilidad de los repositorios institucionales.

Obligaciones de los colaboradores:

- Evitar divulgar y/o transferir la información sensible almacenada en los repositorios institucionales a personas no autorizadas.
- El usuario al cual se asigna un equipo de cómputo, es el único responsable del equipo asignado y de la información de la empresa a la que se acceda a través de este.
- Las credenciales asignadas para el acceso a los repositorios institucionales son de uso personal e intransferible.
- La información almacenada en los repositorios institucionales por parte de los procesos debe cumplir con lo establecido en el reglamento de propiedad intelectual resolución 144 del 20 de noviembre de 2013 o en su defecto el que se encuentre vigente.

3.3 Asignación de equipos de cómputo a colaboradores

Generalidades

La información que se almacena en estos repositorios institucionales es la siguiente:

- Información relacionada con el proyecto en ejecución
- Información que este en versión entregadas y final (Informes, presentaciones, planos, hojas trabajo, actas de reunión, entre otros), en general todos los que constituyan un entregable.
- Información que cada proceso considere importante y esté establecida en las tablas de retención documental (TRD) para el desarrollo de sus actividades y/o que deba mantenerse bajo controles de seguridad con su respectivo respaldo y protección, para mitigar el riesgo de pérdida de información o acceso indebido o no autorizado a la misma.

La información que NO se almacena en las unidades de red o carpetas compartidas es la siguiente:

- Información personal, música en cualquier formato, videos, fotos e imágenes cuya propiedad intelectual no sea de la empresa o que vaya en contra de las normas vigentes relacionadas con derechos de autor y privacidad.
- Información cuya procedencia sea desconocida.
- Información que no se considere relevante para la normal ejecución de las actividades de cada proceso debe guardarse en los discos locales (Unidades nombradas con C y/o D) del equipo de cómputo asignado a cada usuario.
- Para solicitar la recuperación de información de la copia respaldo de los repositorios institucionales se realiza la solicitud al área de Tecnologías de la Información y Comunicación a través de la mesa de servicio y la atención de estos requerimientos se hará conforme al Instructivo de Restauración de Backus.

Descripción

El área de Tecnologías de la Información y Comunicación es la encargada de administrar y asignar los equipos de cómputo y periféricos a los colaboradores que requieran estos recursos. Dicha asignación se realiza una vez el departamento de Recursos Humanos notifica la formalización de la relación contractual, el cargo a desempeñar, el nombre del colaborador y el tipo de contrato así como los recursos digitales necesarios.

Justificación

El uso del equipo de cómputo asignado es personal e intransferible, es utilizado para realizar actividades misionales. Por lo tanto, el colaborador asume responsabilidad en forma expresa de su uso o por parte de terceros.

Obligaciones

- El colaborador deberá contar con autorización (para retirar el equipo) del jefe inmediato cuando va a salir de las instalaciones o retiro frecuente del equipo.
- El equipo asignado es entregado al colaborador con las aplicaciones y software requerido de acuerdo al cargo.
- No se permite la instalación de software diferente al que se le entrega con el equipo de cómputo. Es facultad exclusiva de los responsables de Tecnologías de la Información realizar la instalación de software en los equipos de cómputo de la empresa, con el fin de gestionar las licencias de software propiedad de CONCREARMADO LTDA.
- Para la instalación de software especializado o adicional al que se entrega con el equipo de cómputo se hace la solicitud a través de la mesa de servicio al área de Tecnologías de la Información y Comunicación, aun cuando se trate de software con licenciamiento libre.
- No se instalan licencias propiedad del colaborador o de alguna otra entidad sin la autorización del área de Tecnologías de la Información y Comunicación.
- La copia de archivos de música y video en los equipos de la empresa está restringida, únicamente son válidos para uso interno en cumplimiento con el reglamento de propiedad intelectual vigente por la empresa

Responsabilidades de los usuarios y colaboradores

- Cada usuario y colaborador es responsable de conocer, adoptar y acatar esta Política.
- Los funcionarios son responsables por el uso de la información a su cargo y de los dispositivos de almacenamiento externo que emplee para el transporte de dicha información.

- Cada usuario deberá velar porque estos medios de almacenamiento externo estén libres de software malicioso, espía o virus para lo cual deberá realizar una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la empresa por medio del software de protección dispuesto para tal fin.
- Al finalizar la jornada laboral o durante ausencias temporales de los usuarios, estos deben asegurarse de que los escritorios o mesas de trabajo queden despejados. Por lo tanto, todos los documentos deben ser guardados en archivadores, cajones o compartimentos bajo llave.
- Los colaboradores no deben, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, o dañar o alterar los recursos informáticos.
- No se podrán instalar software
- El ancho de banda de la red y la capacidad de almacenamiento son limitados; por lo tanto, los usuarios no deben realizar acciones que malgasten los recursos de información ni utilizarlos para actividades personales que monopolicen los recursos injustamente en detrimento de los demás usuarios.

3.4 Nombres de archivos y carpetas

El proceso de Tecnologías de la Información, establece que los nombres a los archivos y carpetas sean lo suficientemente significativos sin que sea demasiado extenso.

- Longitud máxima para un nombre de archivo, 256 caracteres (un carácter puede ser una letra, número o un símbolo). El único medio de respaldo de la información para los colaboradores es OneDrive, el cual será configurado por el área de Tecnologías de la Información y Comunicación. El nombre del documento comprende toda la ruta. Ejp.
Y:\00 SISTEMA GESTION INTEGRADO\4 Procedimientos_Instructivos\1 Gestión Integral\1.3 Seguridad de la informacion
- Se sugiere un máximo de 5 niveles de carpeta.

4. Monitoreo de responsables de TI

- Todos los eventos realizados sobre los dispositivos de almacenamiento externo, conectados a cualquier equipo de cómputo de la empresa, podrán ser auditados con el ánimo de registrar y controlar las actividades realizadas sobre cada uno de estos, la ubicación y el usuario que los empleó.
- Los intentos de habilitar el uso de estos dispositivos donde su uso ha sido denegado o no autorizado igualmente podrán ser registrados.
- Las entradas de software malintencionado, de espionaje o virus podrán ser detectadas inmediatamente e informadas al administrador de la red de la empresa.
- Se podrán generar informes periódicos sobre el uso de estos elementos en la empresa para permitir la evaluación del "uso racional de estos dispositivos" donde estos sean permitidos, a fin de incrementar los niveles de seguridad para proteger la información de CONCREAMADO LTDA.

FIRMAS EN DOCUMENTO ORIGINAL

Fernando Amar Garzón
Representante Legal
Gerente General

Fecha	Versión	Revisión	Descripción del Cambio
2024-01-11	0	N.A.	Generación Inicial