# Política corporativa de seguridad de la información

Versión: 4

11-06-2019

dacartec
SERVICIOS INFORMÁTICOS

# Contenido

# CONTROL DE CAMBIOS

| Fecha | Versión | Descripción | Autor |
|---|---|---|---|
| 05/10/2010 | 1.0 | Versión inicial del documento | David Paz Gil |
| 19/11/2018 | 2.0 | Actualización datos | Felipe Hernández |
| 20/05/2019 | 3.0 | Revisión | Iván Rodríguez |
| 11/06/2019 | 4.0 | Revisión | Iván Rodríguez |

# 1. Diagrama de flujo

No aplica

# 2. Objeto

Establecer las normas y requisitos de seguridad que permitan garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información de la Dacartec Servicios Informático (a partir de ahora DACARTEC).

La Política de Seguridad de la Información es un documento que denota el compromiso de la gerencia con la seguridad de la información y debe contener la definición de la seguridad de la información bajo el punto de vista de la entidad.

# 3. Alcance

Este procedimiento aplica a todos los trabajadores de la empresa, así como a aquellos que están subcontratados en DACARTEC.

# 4. Desarrollo

En DACARTEC la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, DACARTEC implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en DACARTEC; este proceso será liderado de manera permanente por el Responsable de Sistemas.

Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

## Políticas generales de seguridad de la información

DACARTEC ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la empresa en cuanto a la protección de sus activos de información:

1. El departamento de sistemas será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de DACARTEC.

2. Los activos de información de DACARTEC, serán identificados y clasificados para establecer los mecanismos de protección necesarios.

3. DACARTEC definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la empresa.

4. Todos los trabajadores serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de DACARTEC.

6. Únicamente se permitirá el uso de software y hardware autorizado que haya sido adquirido legalmente por la Empresa.

7. Es responsabilidad de todos trabajadores de DACARTEC reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

8. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

9. DACARTEC contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

Adicionalmente DACARTEC cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

## Acuerdos de confidencialidad

Todos los trabajadores de DACARTEC y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Empresa, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.
Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de DACARTEC a personas o entidades externas.
Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

## Riesgos relacionados con terceros

DACARTEC identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.
Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

## Uso adecuado de los activos

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la

competencia del área o dependencia específica y a los permisos y niveles de acceso de los trabajadores y contratistas determinadas por los Jefes de proyecto o departamento.
Para la consulta de documentos cargados en el software de Gestión Documental se establecerán privilegios de acceso a los trabajadores y/o contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el jefe del proyecto, quien comunicará al grupo encargado de la administración del software el listado con los trabajadores y sus privilegios.

Todos los trabajadores y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "acuerdo de confidencialidad de la información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerado como un "incidente de seguridad".

## Acceso a Internet

Internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de DACARTEC, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, las siguientes normas:

a) No está permitido:

El acceso a páginas relacionadas con pornografía, drogas, alcohol y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

El acceso y el uso de servicios interactivos, mensajería instantánea, redes sociales y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de DACARTEC.

El intercambio no autorizado de información de propiedad de DACARTEC, de sus clientes y/o de sus trabajadores, con terceros.

La descarga, uso, intercambio y/o instalación de juegos, música, películas, información y/o productos que, de alguna forma, atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica, entre otros.

b) DACARTEC puede realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los trabajadores y/o terceros. Asimismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación vigente.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y las normas de seguridad de la información, entre otros.

d) Los trabajadores y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de DACARTEC, posiciones personales en encuestas de opinión, foros u otros medios similares.

El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de DACARTEC.

## Correo electrónico

Los trabajadores y terceros autorizados a quienes DACARTEC les asigne una cuenta de correo deberán seguir las siguientes normas:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del DACARTEC, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b) Los mensajes y la información contenida en los buzones de correo son propiedad del DACARTEC y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de los buzones de correo es determinado por el Departamento de Sistemas de acuerdo con las necesidades de cada usuario y previa autorización del Jefe correspondiente.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por Departamento de Sistemas

e) No está permitido:

Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Empresa, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

Utilizar la dirección de correo electrónico de DACARTEC como punto de contacto en comunidades interactivas de contacto social, tales como *Facebook* entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

f) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que DACARTEC proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

g) El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la dirección o en su lugar del responsable. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre del departamento respectivo y/o servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

h) Toda información de DACARTEC generada con los diferentes programas (Ej. Office, Project, Access, etc.), que requiera ser enviada fuera de la entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el Departamento de Sistemas.

i) La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

j) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por DACARTEC y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

## Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por DACARTEC a sus trabajadores y/o terceros se reglamenta bajo las siguientes normas:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de DACARTEC es responsabilidad del Departamento de Sistemas, y por tanto son los únicos autorizados para realizar esta labor.

b) Los usuarios no deben realizar cambios en los ordenadores o portátiles relacionados con la configuración del equipo, tales como conexiones de red,

usuarios locales de la máquina, entre otros. Estos cambios pueden ser realizados únicamente por el Departamento de Sistemas.

c) El Departamento de Sistemas debe definir y actualizar, de manera periódica, la lista de software, hardware y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los ordenadores o portátiles de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d) Únicamente los trabajadores y terceros autorizados por el Departamento de Sistemas, previa solicitud, pueden conectarse a la red inalámbrica de DACARTEC.

e) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de DACARTEC, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el Departamento de Sistemas.

f) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de DACARTEC; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos por el Departamento de Sistemas.

g) La sincronización de dispositivos móviles, tales como tablets, smartphones u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la organización, debe estar autorizado de forma explícita por el departamento del usuario, en conjunto con el Departamento de Sistemas y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.

## Control de acceso físico

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás

infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

## Protección y ubicación de los equipos

Los equipos que hacen parte de la infraestructura tecnológica de DACARTEC tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

## Segregación de funciones

Toda tarea en la cual los trabajadores tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

En concordancia:

Todos los sistemas de disponibilidad crítica o media de la empresa deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

## Protección contra software malicioso

DACARTEC establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de este a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad el Departamento de Sistemas autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.
Así mismo, DACARTEC define las siguientes normas:

No está permitido:

La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por DACARTEC.

Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

## Copias de respaldo

DACARTEC debe asegurar que la información con cierto nivel de clasificación, definida en conjunto el Departamento de Sistemas y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la empresa, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, portátiles, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El Departamento de Sistemas establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con los departamentos los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios digitales que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

## Gestión de medios removibles

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, tablets, móviles, cintas) sobre la infraestructura para el procesamiento de la información de DACARTEC, estará autorizado para aquellos trabajadores cuyo perfil del cargo y funciones lo requiera.

El Departamento de Sistemas es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de DACARTEC sólo los trabajadores autorizados pueden hacer uso de los medios de almacenamiento removibles.

Asimismo, el trabajador se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de DACARTEC que éste contiene.

## Intercambio de información

DACARTEC firmará acuerdos de confidencialidad con los trabajadores, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la empresa. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo trabajador de DACARTEC es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

## Control de acceso lógico

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de DACARTEC debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por los diferentes departamentos de la empresa, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica de DACARTEC asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por el Departamento de Sistemas de DACARTEC.
La autorización para el acceso a los sistemas de información debe ser definida y aprobada por el departamento propietario de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los trabajadores y terceros e implementada por el Departamento de Sistemas.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de DACARTEC, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

## Gestión de contraseñas de usuario

Todos los recursos de información críticos del DACARTEC tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada trabajador requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por el Departamento de Sistemas.
Todo trabajador o tercero que requiera tener acceso a los sistemas de información de DACARTEC debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la organización.
El trabajador debe ser responsable por el buen uso de las credenciales de acceso asignadas.

## Escritorio y pantalla limpia

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los trabajadores de DACARTEC deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de

almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

## Segregación de redes

La plataforma tecnológica de DACARTEC que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El Departamento de Sistemas es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

DACARTEC establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la organización.

Es responsabilidad de los administradores garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

## Identificación de requerimientos de seguridad

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en DACARTEC, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad del Departamento de Sistemas y las dependencias propietarias del sistema en cuestión.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre DACARTEC y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad del Departamento de Sistemas garantizar la definición y cumplimiento de los requerimientos de seguridad de la información y en conjunto con la dirección establecer estos aspectos con las obligaciones contractuales específicas.

## 5. Registros

No aplica.

## 6. Anexos

No Aplica