POLÍTICAS INSTITUCIONALES SEGURIDAD INFORMÁTICA

Tomado de
VAF-PI-001-UDES
Versión 18

6.3.2 Lineamientos Generales

a.Estos lineamientos **aplican al personal** administrativo, académico, contratistas, consultores internos, externos y otros trabajadores **que tengan contacto con la información perteneciente a la Universidad de Santander.**

b.Todos los recursos informáticos proporcionados por la Universidad de Santander son propiedad exclusiva de la misma. **Cualquier información almacenada** por los usuarios en los diferentes recursos, **es propiedad de la UDES y no deberán ser eliminados, copiados o compartidos con personas ajenas** a la UDES sin justificación o previa autorización.

c.Todos los equipos de cómputo disponibles en la Universidad para uso en actividades académicos, administrativas, con sistema operativo Windows, **deberán estar incluidos en el dominio de la Institución.**

d.Todos los equipos de cómputo de la Universidad deben tener instalado un antivirus corporativo, si los recursos de hardware no tienen la capacidad de soportar ese antivirus, contarán con el antivirus nativo del sistema operativo, el cual debe estar autorizado por el líder del subproceso de Servicio a Usuario.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

POLÍTICAS INSTITUCIONALES SEGURIDAD INFORMÁTICA

Tomado de
VAF-PI-001-UDES
Versión 18

6.3.2 Lineamientos Generales

e.El usuario es responsable de ejercer el uso apropiado de los recursos informáticos de conformidad con las políticas y directrices de la Gestión TIC.

f.Los servicios de la red institucional de la Universidad de Santander **son de exclusivo uso académico, de investigación, técnicos y para gestiones administrativas.**

g.Los administradores de los servidores institucionales que están a su cargo **son los responsables de la seguridad de la información.**

h.El subproceso de Seguridad Informática entregará directrices a los diferentes administradores de los servidores institucionales, **sobre buenas prácticas** para respaldar la información y configuraciones de seguridad para el servicio ofrecido, de acuerdo con la caracterización de la información.

i.El subproceso de Seguridad Informática es el responsable de respaldar la información almacenada en los equipos informáticos de los usuarios de acuerdo con la caracterización de la información.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

POLÍTICAS INSTITUCIONALES SEGURIDAD INFORMÁTICA

Tomado de
VAF-PI-001-UDES
Versión 18

6.3.2 Lineamientos Generales

j.Todo usuario de la red institucional de la Universidad de Santander **gozará de absoluta privacidad** sobre su información o la información que provenga de sus acciones, **salvo en casos en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional,** sus servicios o cualquier otra red ajena a la Universidad.

k.Cualquier usuario que encuentre o considere que existe una falla de seguridad en los sistemas informáticos de la Institución, **está obligado a reportarlo** a los administradores del sistema o al subproceso de Seguridad Informática.

l.Los usuarios no deben acceder a los datos, documentos, correos electrónicos y los servidores de la UDES **a los que no tienen autorización.**

m.Las actividades relacionadas con la Seguridad Informática, auditorías y mantenimiento **solo pueden ser realizadas por personal autorizado** por el subproceso de Seguridad informática.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.2 Lineamientos Generales

n.Cuando las estaciones de trabajo estén encendidas, pero el usuario deba ausentarse de su puesto de trabajo o esté realizando otras actividades que no incluyan la interacción con el equipo, **la pantalla deberá estar bloqueada con la opción Windows + L o se debe cerrar la sesión,** actividad que es responsabilidad del usuario.

o.El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (bloqueo de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

p.Las nuevas aplicaciones o desarrollos institucionales deben ofrecer protocolos de autenticación LDAP (Directorio Activo), simplificando el acceso con usuarios y contraseñas centralizadas.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

POLÍTICAS INSTITUCIONALES SEGURIDAD INFORMÁTICA

Tomado de
VAF-PI-001-UDES
Versión 18

6.3.3 Cuentas de Usuario (su uso y privacidad)

a.Todos los accesos a los diferentes sistemas de la UDES **son controlados mediante credenciales de usuario y contraseña**, las cuales son de responsabilidad y uso exclusivo del usuario al cual han sido asignadas.

b.Si se requiere hacer uso de los sistemas institucionales, se solicitará formalmente al administrador del sistema correspondiente, **las credenciales de acceso.**

c.La longitud mínima de caracteres permisibles en una contraseña se establece en 8 caracteres y la longitud **máxima de caracteres permisibles en una contraseña se establece en 16 caracteres,** siendo esta una **combinación alfanumérica, mayúscula y minúscula.**

d.Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta sea guardada en un lugar seguro.

e.El subproceso de Seguridad Informática velará por la privacidad de las comunicaciones institucionales, para lo cual monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

POLÍTICAS INSTITUCIONALES SEGURIDAD INFORMÁTICA

Tomado de
VAF-PI-001-UDES
Versión 18

6.3.3 Cuentas de Usuario (su uso y privacidad)

f.El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.

g.El usuario es responsable exclusivo de mantener a salvo su contraseña. Los usuarios no deben compartir su(s) cuenta(s), contraseñas, números de identificación personal (PIN), tokens de seguridad, información similar o dispositivos utilizados para propósitos de identificación y autorización.

h.Está permitido el uso de la herramienta KeePass para administración de contraseñas, permitiendo la centralización de las mismas a una única fuente, minimizando el riesgo de pérdida de credenciales. Esta aplicación está autorizada por el subproceso de Servicio a Usuario, responsable de la instalación a solicitud del interesado.

i.Al compartir documentos en nube (OneDrive), el usuario creador es responsable de asignar los permisos para visualizar, editar o borrar el archivo o documento, según aplique, **con el fin de asegurar el buen uso de los elementos compartidos.**

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

POLÍTICAS INSTITUCIONALES SEGURIDAD INFORMÁTICA

Tomado de
VAF-PI-001-UDES
Versión 18

6.3.4 Uso de Correo Electrónico

a.Los correos electrónicos que sean enviados o recibidos bajo los dominios institucionales: udes.edu.co, cucuta.udes.edu.co, campus.udes.edu.co, valledupar.udes.edu.co, mail.udes.edu.co, **serán de uso exclusivo de la Institución.**

b.Los usuarios deben reportar al Subproceso de Seguridad Informática **todos los casos de mensajes de correos basura,** tales como distribución de **material ilegal u ofensivo, ataques de phishing, entre otros.**

c.Está prohibido el envío de correo electrónico de pornografía de cualquier tipo, propaganda política **o cualquiera que discrimine a una o varias personas.**

d.En caso de que un usuario detecte que se haya leído y/o entrado a su información o cuentas de correo de su computadora sin la respectiva autorización, **deberá notificar a Seguridad Informática.**

e.No registrar los correos corporativos a foros y páginas que generen envío de publicidad a menos que sea para fines laborales, académicos o investigación.

f.El usuario es responsable del buen uso del envío de correo electrónico y la calidad de la base de datos utilizada, evitando enviar correos a destinatarios con cuentas inactivas, ocasionando que su cuenta se pueda reportar como Spam.

g.Para envío de correos masivos se debe realizar por los subprocesos autorizados existentes.

6.3.5 Manejo y Seguridad de Medios de Almacenamiento y Dispositivos Extraibles

a.En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, **de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información**, por ende, **el usuario responsable de la estación o terminal de trabajo no debe utilizar medios de almacenamiento extraíbles**

b.Para el respaldo de la información institucional no se deben utilizar medios de almacenamiento extraíbles, toda vez que pueden facilitar el robo o manipulación de la información por terceros o personal no autorizado. **Las copias de seguridad deben hacerse en sistemas de respaldo centralizados, administrados por el subproceso de Seguridad Informática**. En casos excepcionales, podrá autorizarse el uso de estos dispositivos temporalmente.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.5 Manejo y Seguridad de Medios de Almacenamiento y Dispositivos Extraibles

c.En casos excepcionales, cuando se utilicen dispositivos de almacenamiento extraíbles tales como: USB, Discos duros portátiles, CD, **DVD el usuario debe tomar las precauciones necesarias** verificando con programas antivirus que dichos dispositivos se mantienen libre de virus o cualquier otra amenaza. **Se debe tener en cuenta que el daño o pérdida de información por manipulación del medio de almacenamiento, es responsabilidad del usuario.**

d.La utilización de medios de almacenamiento extraíbles personales esta totalmente prohibido por la Universidad de Santander

e.La utilización de medios de almacenamiento extraíbles (corporativos) está sujeta a la autorización del subproceso de seguridad informática.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.6 Consideraciones sobre auditorías de Seguridad Informática

a.Cualquier acción que amerite la ejecución de una auditoría a los sistemas informáticos, deberá ser documentada y establecida su aplicabilidad y objetivos de la misma, así como razones para su ejecución, personal involucrado en la misma y sistemas implicados.

b.La auditoría **no deberá modificar** en ningún momento el sistema de archivos de los sistemas implicados, **en caso de haber necesidad de modificar algunos se deberá hacer un respaldo formal del sistema o sus archivos.**

c.Las auditorías que se realicen deben estar enmarcadas dentro de lo establecido en el Programa de Auditorías VAF-PG-002-UDES. Estas auditorías serán realizadas por personal de Seguridad Informática o por personal asignado por la Vicerrectoría Administrativa y Financiera.

d. En caso de emergencia, **solamente el personal del subproceso de Seguridad Informática serán los encargados de hacer rastreo de toda la data y del informe de forense.**

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.6 Consideraciones sobre auditorías de Seguridad Informática

e.Está prohibido para cualquier usuario, interceptar paquetes de datos, modificar, leer (utilizando elementos tales como sniffers, SNMP, RMON, NMAP y otros) los datos electrónicos privados (ya sea en tránsito a través de la red o almacenados dentro de una computadora) **sin el consentimiento escrito del propietario legítimo.**

f.Solo personal autorizado por la Vicerrectoría Administrativa y Financiera, se le permitirá modificar, eliminar, leer datos electrónicos (ya sea en tránsito a través de la red o almacenados dentro de una computadora)**.**

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.7 Acceso a Red o Uso de Internet

a.El acceso a la navegación de Internet está controlado mediante perfiles web clasificados en páginas seguras, productivas y no productivas. **Los perfiles serán ajustados según el área de trabajo, con previa autorización del jefe inmediato**.

b.No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

c.No está permitido el acceso y el uso de servicios P2P como ares, Kazaa, emule y otros similares, **que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades** propias de la Universidad de Santander.

d.Está prohibido descargar de manera fraudulenta archivos protegidos por la propiedad intelectual de derecho de autor, cualquier descarga será responsabilidad total de la persona que realiza la misma y vendrá sujeto a sanciones.

e.El área de Seguridad Informática realizará el monitoreo permanente de: tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.7 Acceso a Red o Uso de Internet

f.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 los lineamientos de seguridad de la información, entre otros.

g.Para **la conexión a las aplicaciones o servidores** se debe realizar por comunicaciones seguras como protocolos SFTP, SSH, HTTPS.

h.Para realizar conexión remota a los equipos corporativos se debe efectuar por mecanismos seguros como VPNS (Ipsec o SSL), estos accesos deben tener autorización del líder del proceso académico, administrativo y de Talento Humano para trabajo remoto.

i.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 la Universidad de Santander.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.8 Red Inalámbrica

a.Está prohibida la interceptación de las comunicaciones y la utilización de técnicas de escucha de cualquier señal de comunicaciones sin la previa autorización por parte de la Dirección de Tecnologías de la Información y las Comunicaciones.

b.No se debe realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de estos intentos no autorizados es una práctica ilegal y no es permitido por la Institución.

c.Toda información transferida a través de este medio viaja de manera INSEGURA, la Dirección de Tecnologías de la Información y las Comunicaciones (TIC) no es responsable por el robo de la información a través de este tipo de conexión.

d.La Dirección de Tecnologías de la Información y Comunicaciones (TIC) podrá suspender o desactivar temporalmente el servicio o cancelarlo de manera definitiva para determinado equipo, cuando detecte que el usuario haya hecho uso indebido del servicio. La reactivación deberá ser autorizada por Vicerrectoría de Enseñanza para el caso de alumnos y profesores, y por la Vicerrectoría Administrativa y Financiera para el caso de usuarios administrativos y externos.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.8 Red Inalámbrica

e.La Dirección de Tecnologías de la Información y las Comunicaciones (TIC) está facultada para realizar rastreos periódicos, análisis de tráfico y los controles que considere necesarios para mantener la operación de la red inalámbrica en buen estado y detectar usos indebidos del servicio. A solicitud escrita de la autoridad competente o cuando exista alguna orden judicial para responder ante procesos legales, la Dirección de TIC proporcionará la información transmitida en la red inalámbrica que esté disponible para su acceso de conformidad con las leyes aplicables.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196

6.3.9 Centro de Cableado o Datacenter

a.Los ingresos a los centros de cableado y datacenter se debe realizar por medio de control de acceso ya sea por tarjeta de proximidad RFID o por medios de llaves.

b.El acceso al datacenter debe ser controlado por medio de una bitácora de visitas.

c.Mantener los centros de cableado y datacenter libres de elementos inflamables como cajas, cartones, entre otros.

d.Retirar todo material magnético (ferromagnético, diamagnético, paramagnético,) **dado que pueda dañar las unidades de almacenamiento.**

e.Mantener el área limpia y ordenada.

Bucaramanga
seguridadinformatica@udes.edu.co
(607) 6516500 **Ext**. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
(605) 5730073 **Ext.** 129

Cúcuta
wpena@udes.edu.co
(607) 5748717 **Ext.** 4196