A.13 Seguridad de las comunicaciones (POL-09)

A.13 Seguridad de las comunicaciones (POL-09)

1. Objetivo

Establecer las directrices para garantizar la protección de la información en las redes e infraestructura de apoyo para el procesamiento de información de la organización.

2. Alcance

Es de aplicación para toda la organización para la seguridad de las comunicaciones.

3. Política

A.13.1 Gestión de Seguridad en la red

A.13.1.1 Controles de red

- La Administración Técnica de Seguridad de la Información (ATSI) debe cumplir con los siguientes puntos en la administración y configuración:

  - Todos los dispositivos de comunicación deben tener configuradas contraseñas para acceder a las funciones de operación y administración.
  - Se deben restringir las actividades y funciones que puedan realizar los operadores y los administradores sobre las plataformas de cómputo y comunicaciones de acuerdo a su perfil.
  - El acceso a las funciones de operación y administración de los dispositivos de comunicación se debe realizar exclusivamente a través de una consola específica o de terminales restringidas.
  - Los servicios de File Transfer Protocol (FTP) en los equipos de comunicación se deben habilitar de acuerdo a los perfiles de usuario documentando los mismos. De igual manera, se deben deshabilitar todos los servicios o protocolos que no sean requeridos.

A.13.1.2 Seguridad en los servicios de red

- Se debe monitorear y proteger los servicios de red en contra de accesos no autorizados para lo cual debe cumplir con los siguientes puntos:

  - Identificar y documentar las redes y servicios de red utilizados por usuarios.
  - Definir procedimientos de autorización para determinar qué usuarios pueden acceder las redes y los servicios de red.
  - Los privilegios de acceso otorgados a los usuarios sólo deben incluir aquellos que están explícitamente autorizados a utilizar.
  - Se debe identificar, implementar y mantener los mecanismos y procedimientos de monitoreo de servicios de red que permitan identificar como mínimo a nivel usuario o grupo de usuarios:

    a) Accesos a los servicios de red.
    b) Intentos de acceso no autorizados.
    c) Cambio de privilegios especiales no autorizados.

- El Administrador Técnico de Seguridad de la Información debe controlar los accesos permitidos a los sistemas de administración y monitoreo, y vigilar estrechamente las actividades relacionadas, almacenándolas en bitácoras.

A.13.1.3 Segregación en redes x

A.13.1.3.1 Administración del internet

- El ATSI debe limitar a usuarios el acceso a los servicios de Internet de acuerdo a los propósitos exclusivamente autorizados por la organización.
- El ATSI debe revisar y monitorear el uso de los servicios, equipos, información enviada o recibida, intentos de ataques y vulnerabilidades de los sistemas utilizados, a fin de reducir los riesgos derivados del uso de Internet.
- La organización deberá contar con 3 segmentos de red: el primero designado a las operaciones inalámbricas (Wi-Fi), el segundo segmento estará dedicado exclusivamente a los servicios administrativos de la empresa y el tercer segmento a los servicios operativos.

A.13.1.3.2 Control del uso de internet

- La Alta Dirección se reserva el derecho de bloquear el acceso a ciertos sitios de web que no estén relacionadas con funciones propias de la organización.
- El ATSI debe crear y mantener los procesos y mecanismos que permitan la autorización y control de usuarios con derecho de uso y acceso a Internet.
- El acceso a los servicios de Internet debe realizarse exclusivamente a través de los equipos y medios de comunicación expresamente autorizados.
- Aplicaciones ajenas deben ser aprobados por el ATSI.
- Todos los usuarios que utilicen el servicio de Internet pertenecientes a la organización, deben hacerlo de manera responsable.
- Queda prohibido conectarse a redes inalámbricas no administradas por la organización dentro de las instalaciones.
- Queda explícitamente prohibido el uso de internet para las siguientes actividades:

  - Descargar software ilegal o para uso personal.
  - Descargar música y/o videos de manera ilegal.
  - Realizar “streaming” desde las instalaciones de la organización.
  - Utilizar software P2P.
  - Subir información confidencial y/o reservada en repositorios no autorizados por la organización.

A.13.2 Transferencia de información

A13.2.1 Políticas y procedimientos de transferencia de información

- Todos los acuerdos y procedimientos de transferencia de información que deben seguirse, están estipulados en los siguientes puntos del apartado A.13.2 de la presente política y en el **Proceso de comunicación (PRO-02).**
- Todo medio de almacenamiento extraíble (USB, disco duro, CD, DVD, memorias SD o microSD), deberán estar cifradas antes de salir de las instalaciones de Digilogics de acuerdo a la política **A.10 Criptografía (POL-06).**

A.13.2.2 Acuerdos de transferencia de información

- Se debe incluir la siguiente leyenda en la firma de correo electrónico:

  “A partir del presente comunicado, los medios de contacto serán a través de correo electrónico y/o teléfono mencionado en la firma del presente correo”.

- Los acuerdos de intercambio de información que establezcan, deben considerar como mínimo los siguientes aspectos:

  - Definición del medio para la transferencia de la información.
  - Definición de responsabilidades por divulgación o pérdida de información por medio de la firma de un Convenio de confidencialidad entre las dos partes. En las cláusulas primera, segunda,

tercera y cuarta del documento **Modelo de Convenio de confidencialidad (PRO-10.FO-03)**, se especifican dichas responsabilidades antes mencionadas y sus excepciones.

A.13.2.3 Mensajería electrónica

- El correo electrónico es exclusivamente para actividades de trabajo relacionadas con la organización.
- Queda explícitamente prohibido el uso del correo electrónico para las siguientes actividades:

  - Distribución y explotación de información confidencial de la organización sin previo consentimiento o autorización del gerente y/o director del área dependiendo del nivel de clasificación de la información a enviar.
  - Actividades Ilícitas.
  - Fines de lucro ajenos a la organización.
  - Acoso y con fines racistas.
  - Fines personales.
  - Entretenimiento.
  - Envío de propaganda.
  - Contenido sexual explícito.

- Los usuarios deben borrar, sin abrir, todos los correos electrónicos que procedan de cuentas de correo que les sean desconocidas o cuyo "asunto" pueda relacionarse con publicidad o virus.
- Todos los correos electrónicos que se emitan desde cuentas de correo de la Institución deben contar con la leyenda:

  NOTA: La información de este correo y sus archivos adjuntos es de propiedad exclusiva y confidencial del emisor. Este mensaje es sólo para el destinatario señalado, si usted no lo es, destrúyalo de inmediato. Ninguna información aquí contenida debe ser entendida como dada o avalada por DIGILOGICS, S.A. de C.V, o sus empleados, salvo cuando ello expresamente se indique. DIGILOGICS S.A. de C.V. o sus empleados, no serán responsables por la recepción o propagación de virus, es responsabilidad del receptor contar con una herramienta para la revisión de correos electrónicos.

4. Control de Versiones

Número de Versión	Fecha de Actualización	Descripción del Cambio
3.0	Marzo, 2021	Actualización de los controles A.13.1.2, A.13.1.3, A.13.2.1, A.13.2.2 y A.13.2.3