1. DESARROLLO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL USO DE VPN

1.1. INTRODUCCIÓN1

En cumplimiento de las Políticas de Seguridad y privacidad de la información de IDEAM, y siguiendo lineamientos institucionales respecto a la protección y uso adecuado de los activos de información, se definen las directrices necesarias para acceder a los servicios tecnológicos de la entidad por medio de conexión por VPN, teniendo en cuenta el "**Plan de seguridad y privacidad de la información IDEAM - Política 6. soporte y mantenimiento a hardware, software, bases de datos, dispositivos de seguridad perimetral, redes y comunicaciones"**, en lo referente a la habilitación y/o creación de VPN en la entidad, se establece lo siguiente: Los accesos a servicios tecnológicos del IDEAM por parte de los funcionarios, contratistas, terceros y/o proveedores por medio de internet, a excepción del servicio FTP, deberán realizarlos por conexión segura, denominada Virtual Private Network – VPN de tipo VPN Client to Site, la cual se caracteriza por el acceso a recurso(s) especifico(s) por parte de los usuarios.

1.2. OBJETIVOS

OBJETIVO GENERAL

Definir lineamientos para gestionar de forma oportuna el acceso a los recursos de TI de IDEAM mediante la conexión de Redes Virtuales Privadas VPN, que permitan propender por los principios de Confidencialidad, Integridad y Disponibilidad de la información.

1.3. ALCANCE

El presente documento está dirigido a toda la entidad a nivel nacional, orientando sobre el proceso de solicitud de VPN a los funcionarios, contratistas, terceros y/o proveedores, además de las políticas de seguridad de la información para tal fin.

1.4. DEFINICIONES

Aplicación: Es un tipo de programa informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo

Administración: Creación, actualización, modificación o eliminación de algún recurso, entidad, u objeto involucrado en un Sistema de Información.

Contratista: Persona jurídica o natural externa al Instituto encargada de adelantar actividades por encargo del instituto.

Cuenta de acceso: Identificación y contraseña a través de la cual un usuario accede a un servicio o aplicación. Las cuentas de acceso son autorizadas por los jefes de las diferentes dependencias y suministradas por los Administradores de los servicios o aplicaciones y está sujeta a la disponibilidad de licencias adquiridas por el Instituto.

Dependencia Solicitante: Área ubicada dentro del organigrama del IDEAM; que requiere de los servicios de la Oficina de Informática. Ejemplo: Áreas Operativas, Subdirección de Hidrología, etc.

Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.

Incidente de Seguridad de la Información: Un incidente de seguridad de la información se define como cualquier evento que compromete o afecta potencialmente el ambiente de seguridad de la información de una organización, en cualquiera de sus principios de confidencialidad, integridad o disponibilidad.

Información: Es un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados o estructurados en un contexto determinado tienen algún significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo, la información es considerada como un activo con valor incalculable, esencial para las actividades del instituto.

Integridad: Salvaguarda de la exactitud y completitud de la información y sus métodos de procesamiento.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Servicio o Aplicación: Programa o conjunto de programas diseñados para la realización de una(s) tarea(s) concreta(s). Los servicios están destinados principalmente para apoyar los diferentes procesos del Instituto. Por ejemplo, correo electrónico, Internet, SISAIRE, SNIF, SIORH, etc.

Recurso Informático: Cualquier componente físico (Hardware) o lógico (Software) empleado para almacenar, manipular, procesar o transmitir información del IDEAM.

Usuario: Es la persona que utiliza un producto o servicio con algún propósito específico

VPN: Red Virtual Privada.

1.5. POLÍTICAS DE OPERACIÓN

A continuación, se especifican las políticas de operación para la solicitud y uso de conexiones VPN.

Se deberán implementar controles de acceso que permitan verificar la identidad de los usuarios autorizados para establecer la conexión por medio de VPN y así mismo restringir el acceso a aquellos que no estén autorizados.

La transmisión de la información durante la conexión por VPN, deberá incluir controles criptográficos, con el fin que no pueda ser expuesta o leída por personal no autorizado.

Proceso De Solicitud De Servicio De VPN.

TIPO DE CONEXIÓN VPN	DESCRIPCIÓN	AUTORIZADOS	FORMATO DE SOLICITUD
SITE TO SITE	Permite interconectar de forma segura dos o más Redes de comunicaciones en diferentes ubicaciones físicas, su enfoque está orientado a brindar soluciones corporativas mediante la interoperabilidad entre varias compañías que disponen de oficinas, sucursales en diferentes ubicaciones físicas.	Conexión especial en caso de interconectar y/o interoperar con otra entidad u organización.	E-GI-F032 FORMATO SOLICITUD DE CONEXIÓN VPN SITE TO SITE
VPN CLIENT TO SITE	Permite establecer una conexión segura y privada para acceder a los recursos institucionales de TI, como si se estuviera directamente en las instalaciones, manteniendo funcionalidad y seguridad de IDEAM.	Funcionarios, contratistas y personal que la entidad lo determine.	E-GI-F031 FORMATO SOLICITUD DE CONEXIÓN VPN CLIENT TO SITE

Este servicio deberá ser solicitado por los jefes de dependencia, mediante proceso oficial de inscripción de caso en la mesa de servicio institucional diligenciando y anexando al mismo, el formato establecido según el tipo de solicitud.

Los formatos están disponibles en el Sistema de Gestión Integrado – SGI en la intranet bajo el proceso "**Gestión de tecnología de información y comunicaciones**".

Una vez aprobada la conexión, se remitirá el instructivo al usuario para la configuración de la misma en el computador remoto.

La conexión por VPN asignada será monitoreada directamente desde la Oficina de Informática.

La conexión por VPN únicamente será autorizada y habilitada en caso de que el usuario requiera acceder a un servicio específico, el cual no se pueda establecer una comunicación externa y este solo esté disponible de forma privada al interior de la Entidad.

1.6. OBLIGACIONES DE USUARIO DE SERVICIOS DE VPN

Únicamente será asignada siempre y cuando el funcionario y/o colaborador dispongan de una cuenta oficial/ usuario de dominio de la entidad además de la aprobación de la solicitud realizada previamente a través de la mesa de servicio.

La asignación de credenciales de acceso deberá cumplir con los requisitos mínimos de seguridad establecidos directamente por la oficina de informática. Las contraseñas deben tener mínimo 8 caracteres, los cuales deben contener letras mayúsculas y minúsculas, números y caracteres especiales: "#$%&/(+/*.

Es responsabilidad del usuario, propender por la confidencialidad y no divulgación de la información institucional, además deberá asegurar que ninguna otra persona manipule los accesos otorgados. Cabe recordar que las credenciales de acceso son de carácter personal e intransferibles y de uso exclusivo de la entidad.

La Oficina de Informática realizará monitoreo a todas las sesiones por VPN. Si se detecta inactividad superior a 10 minutos, por seguridad la conexión expirará y se requerirá que el usuario inicie sesión nuevamente.

- Si durante el monitoreo se observa algún comportamiento inadecuado de la conexión, será evaluado y posteriormente bloqueado esto con el fin de prevenir incidentes que puedan afectar la seguridad de la información y la operación de los servicios de TI.

- El usuario deberá proceder a realizar el cierre de la sesión y desconexión del acceso por VPN cada vez que finalice las labores.

No se permite la instalación, configuración y/o conexión de la VPN desde lugares que no dispongan de controles de seguridad adecuados. Tal es el caso de los equipos de cómputo de lugares públicos (café Internet), salas de conferencia, entre otros.

La conexión con los servicios tecnológicos de la entidad deberá realizarse a través de un computador personal ubicado en la sede del IDEAM correspondiente, el cual deberá estar encendido.

La conexión deberá establecerse únicamente por medio de la herramienta asignada por la Oficina de informática.

La configuración del acceso a los servicios institucionales por medio de la VPN será responsabilidad de cada usuario. Para ello se anexa el instructivo para descarga y configuración de la herramienta que permitirá otorgar el acceso.

1.7. REQUISITOS PARA ACTIVACIÓN DE SERVICIOS DE VPN

Por parte del usuario es indispensable disponer de un servicio de internet, también deberá tener a disposición un equipo de cómputo ya sea portátil y/o escritorio aprovisionado con las características mínimas listadas a continuación:

1.8. Proceso De Solicitud De Servicio De VPN.

TIPO DE CONEXIÓN VPN	DESCRIPCIÓN	AUTORIZADOS	FORMATO DE SOLICITUD
SITE TO SITE	Permite interconectar de forma segura dos o más Redes de comunicaciones en diferentes ubicaciones físicas, su enfoque está orientado a brindar soluciones corporativas mediante la interoperabilidad entre varias compañías que disponen de oficinas, sucursales en diferentes ubicaciones físicas.	Conexión especial en caso de interconectar y/o interoperar con otra entidad u organización.	E-GI-F032 FORMATO SOLICITUD DE CONEXIÓN VPN SITE TO SITE
VPN CLIENT TO SITE	Permite establecer una conexión segura y privada para acceder a los recursos institucionales de TI, como si se estuviera directamente en las instalaciones, manteniendo funcionalidad y seguridad de IDEAM.	Funcionarios, contratistas y personal que la entidad lo determine.	E-GI-F031 FORMATO SOLICITUD DE CONEXIÓN VPN CLIENT TO SITE

2. DOCUMENTOS RELACIONADOS

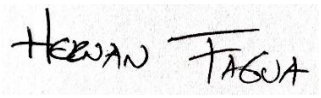
Ningún documento relacionado.

3. BIBLIOGRAFÍA

Ninguna a relacionar. Es documento de autoría única.

4. HISTORIAL DE CAMBIOS

Versión	Fecha	Descripción
1.0	24-03-2020	Documento inicial

ELABORÒ:	REVISÒ:	APROBÒ:
 Hernán Darío Fagua Yanquen Oficial de Seguridad	 Alicia Barón Leguizamón Jefe (E) oficina de Informática	 Alicia Barón Leguizamón Jefe (E) oficina de Informática