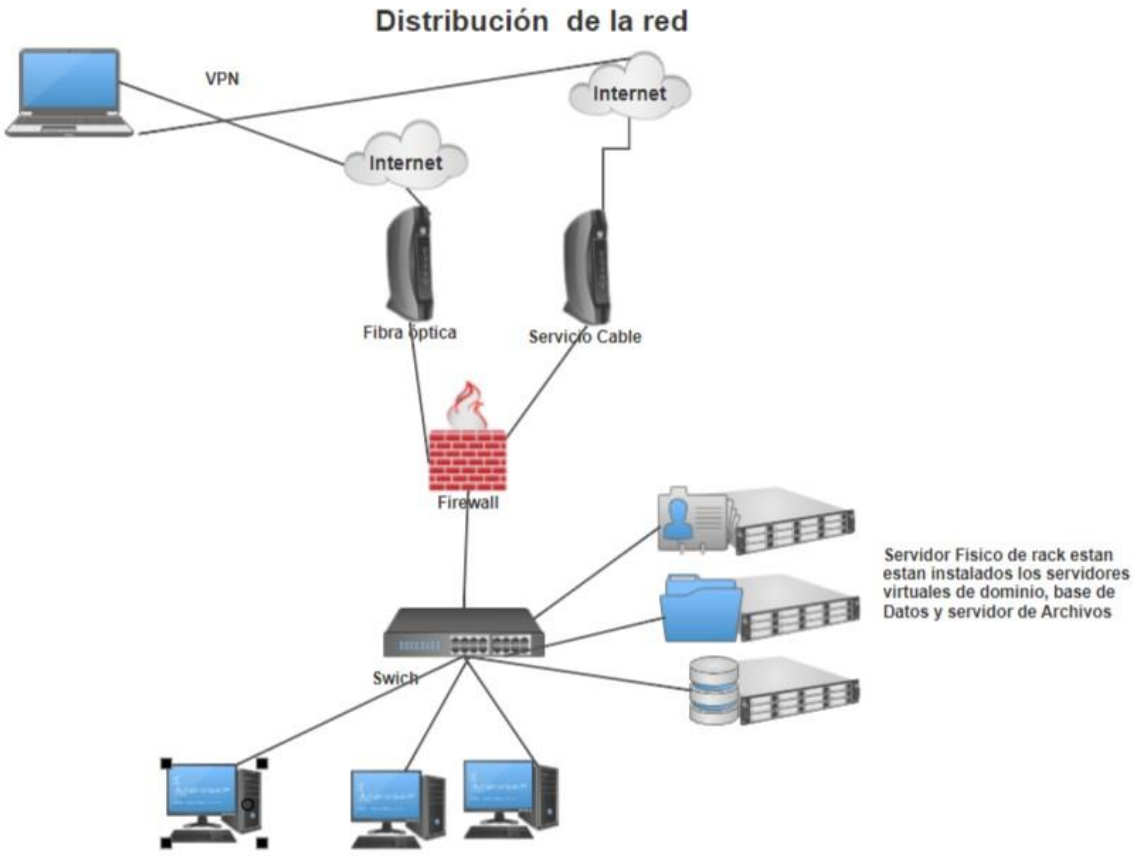
OFICINA NACIONAL DE SEMILLAS

PLAN DE SEGURIDAD INFORMATICA

Versión 1.00

2019-2021



Seguridad a Nivel de Red

Objetivo General

Planificar, orientar y desarrollar los mecanismos necesarios para dotar de confidencialidad e integridad al conjunto de datos y activos de información de la institución

Objetivos Específicos

Formular el esquema de seguridad de la información de acuerdo a las necesidades de los sistemas de información.

Instaurar medidas de control de acceso a los activos de información de la institución.

Establecer las acciones, responsabilidades frente a la garantía de la seguridad de la información de la institución.

1. Firewall Físico

La Oficina Nacional de Semillas cuenta con un firewall Virtual de la empresa Panda con la solución Panda GateDefender Performa eSeries con licenciamiento hasta enero 2022 el cual proporciona el siguiente nivel de seguridad:

1.1. Acceso a Internet seguro y libre de malware

Analiza y protege los protocolos más comunes:

- Filtrado HTTP y HTTPS con Inspección Profunda de Paquetes SSL
- Filtrado de imágenes no apropiadas en navegación mediante tecnología Safesearch
- Protocolos de correo SMTP y POP3
- Descarga de ficheros por FTP

1.2. Cortafuegos y sistema de detección de intrusos

Filtra el tráfico de red entrante y saliente de la organización, bloqueando los accesos no autorizados y permitiendo al mismo tiempo las comunicaciones autorizadas

2. Antivirus y Firewall

Supervisa y clasifica todos los procesos ejecutados en el parque informático en base a su comportamiento y naturaleza. Gracias a este servicio los puestos de usuario y servidores son protegidos limitando la ejecución de los programas instalados a aquellos que han sido previamente certificados como seguros.

La plataforma reside en la nube, es directamente accesible por todos los equipos suscritos al servicio, desde cualquier lugar y en cualquier momento, sin importar si están dentro de la oficina o desplazados.

2.1. Protección

- Protección del correo y la Web
- Protección mediante reglas de sistema
- Protección de programas

- Sistema de detección de intrusos
- Filtrado de Spam, Virus
- Detección de exploits
- Filtrado de la llegada de correo con Phising o Spam

2.2. Control de contenido web

Las políticas de control de contenido web se definen para usuarios comunes o administradores de red.

3. Seguridad Lógica

La seguridad lógica es necesaria para proteger los activos de información de la oficina Nacional de Semillas para que sean siempre utilizados de forma autorizada, por razones de sus funciones, y evitar acciones que puedan provocar su alteración, borrado o divulgación no autorizados, de forma accidental o intencionada.

4. Seguridad ingreso al Dominio

Son usuarios del dominio los funcionarios, y todo aquel que utilice los recursos, aplicaciones y servicios que brinda la Oficina Nacional de Semillas

El Administrador del Dominio será el encargado de crear los usuarios de dominio, previa recomendación de la jefatura administrativa Financiera.

El nombre de usuario del dominio se creará con la inicial del primer nombre y primer apellido, si se repitiere se optará por complementarlo con los otros nombres y apellidos.

Al crear un usuario de dominio, se le asignará una contraseña temporal, Al usuario se le solicitará realizar el cambio de contraseña cuando ingrese por primera con la contraseña temporal, la contraseña contará, mínimo con ocho caracteres alfanuméricos y deberá evitar 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. Debe contener al menos un carácter en minúscula, uno en mayúscula y un número.

Los usuarios asignados a una persona deberán ser únicos e intransferibles, indicando con esto que es la persona titular de dicho usuario quien tiene la responsabilidad de salvaguardar las respectivas contraseñas.

Los usuarios de las aplicaciones deberán tener su usuario y contraseña personal e intransferible y se asignarán previa solicitud de aplicaciones y autorización del jefe inmediato, El usuario y contraseña de la aplicación será asignado por el administrador de la aplicación.

Es responsabilidad del usuario el buen uso del correo institucional, evitando publicar o entregar sus credenciales (usuario y contraseña) ya que estas nunca les serán requeridas, además de evitar caer en las múltiples acciones de ingeniería social para la distribución de virus y correos no deseados. En cualquier caso, de sospecha al momento de recibir correos con situaciones extrañas, el usuario debe informar al administrador de sistemas para evaluar la situación y tomar las medidas pertinentes.

5. Seguridad en el Acceso a la Información

5.1. Identificación de usuarios.

Es el control que permite a un usuario acceder de forma individual a la computadora.

5.1.1. Cada identificador de usuario está asignado a un funcionario, que es responsable de las actividades realizadas por él.

5.1.2. El identificador de usuario se asigna a un funcionario para facilitarle el acceso al sistema de información, se define y utiliza una nomenclatura estándar en la creación de identificadores, de forma que un usuario tenga el mismo identificador en todos los sistemas que necesite utilizar.

5.2. Con este sistema de identificación se consigue:

5.2.1. Utilizar un método de Identificación única, que permita al usuario realizar los procesos de identificación y autenticación una sola vez, en la primera conexión al sistema.

5.2.2. Autorización de Usuarios.

El acceso de cada usuario a los sistemas de la oficina tiene que ser aprobado previamente por el administrador del sistema. Hay definido un procedimiento, manual, para autorizar la inclusión de nuevos identificadores de usuarios en el sistema y que incluya la notificación al administrador responsable del usuario.

5.3. Eliminación de Usuarios.

5.3.1. En caso de terminación de la necesidad de uso por razones de negocio o abandono de la Institución, hay definido un procedimiento, manual, para la eliminación de identificadores de usuarios del sistema. El administrador del usuario es responsable las condiciones de que son motivo dicha eliminación.

5.3.2. El procedimiento incluye los controles para prevenir el acceso de un usuario a los sistemas, inmediatamente después de la comunicación de su director. Un identificador de usuario eliminado, no se volverá a asignar a ninguna otra persona en el futuro.

5.4. Control de contraseñas.

5.4.1. El acceso a la información sensible de la oficina, aplicaciones y sistemas informáticos está regulado contra accesos no autorizados, requiriéndose, dentro del ámbito informático el uso de una clave de usuario y una contraseña para poder acceder a ella.

5.4.2. La contraseña elegida por el usuario será cambiada regularmente, en torno a una vez cada tres meses.

5.4.3. La contraseña no podrá ser vista en ningún momento y en ningún sistema.

5.4.4. El número de intentos de escritura de la contraseña estará limitado a tres intentos, bloqueándose el terminal en caso de superar dicho límite.

5.4.5. La contraseña deberá ser una combinación de números y letras no relacionadas con ningún dato de carácter personal.

5.4.6. Las contraseñas se almacenan en una base de datos encriptada a la que será imposible su acceso, ni siquiera para lectura simple.

5.4.7. La contraseña debe tener una longitud mínima de 6 caracteres, o tener al menos un carácter numérico y uno alfabético.

5.4.8. No contener el identificador de usuario, como parte de la contraseña.

5.4.9. El sistema automáticamente rechazará las contraseñas que no cumplan la normativa.

5.4.10. El personal relacionado con la seguridad dispondrá de procedimientos de recuperación de contraseñas para los casos en los que a los usuarios se les haya olvidado.

5.5. Restauración de contraseñas.

El usuario debe solicitar por escrito la restauración de la contraseña. Está definido e implantado un proceso para asegurar la restauración o cambio de contraseña, por pérdida u olvido de la anterior o cuando se sospeche que es conocida por otra persona.

El proceso incluye la identificación positiva del solicitante o, en caso contrario, Este proceso es automatizado para favorecer la gestión de la contraseña por el propio usuario. Tanto la solicitud como la respuesta se realizan a través de un medio seguro.

6. Protección en terminales.

Todo usuario es responsable de proteger el terminal que le ha sido asignado, y colaborar en la protección de cualquier otro terminal de la oficina, para evitar que sea robado o dañado.

Se congelarán automáticamente los equipos y se bloqueará el uso de estaciones de trabajo, para evitar acciones de personas no autorizadas, si no hay actividad en ellas, durante un periodo superior diez minutos, requiriéndose la entrada de la contraseña para poder desbloquear la estación de trabajo.

Cuando los terminales requieran compartir accesos, por razones de negocio, los procedimientos deberían asegurar que solo las personas con autorización por escrito de la Jefatura administrativa Financiera puedan acceder.

Al finalizar la jornada laboral, se utilizarán los mecanismos de apagado del equipo.

7. Acceso físico al áreas de TI

7.1. En general las oficinas de las Áreas de Tecnologías de Información son de acceso restringido, dadas las características del trabajo que se desarrolla en sus instalaciones.

7.2. Los funcionarios de las diferentes dependencias podrán ingresar a la recepción del de TI, para efectos de solicitar servicios o consultas. Asimismo, podrán ingresar al interno de las oficinas siempre que este el funcionario de TI que los atienda personalmente.

8. Administración y mantenimiento de bases de datos

8.1. Todo mantenimiento a las bases de datos deberá ser realizado por personal técnico capacitado interno o externo, quienes deberán ser supervisados por el profesional responsable de esa tarea de TI.

8.2. Antes de cualquier proceso de mantenimiento a la base de datos, se deberán realizar los respaldos respectivos para estar prevenidos contra cualquier accidente que se pudiera presentar.

8.3. Todo cambio o ajuste hecho en el proceso de mantenimiento, se deberá dejar documentado en una bitácora para efectos de control y seguimiento.

9. Copias de seguridad (backup)

Las copias de seguridad se harán de forma periódica, de todas las bases de datos de la institución en horario 9 p.m.

LUNES	MARTES	MIERCOLES	JUEVES	VIERNES	SABADO	DOMINGO
COMPLETA	COMPLETA	COMPLETA	COMPLETA	COMPLETA		

Copias de seguridad de las máquinas virtuales:

Las máquinas virtuales se respaldan en discos externos una copia diaria y una copia semanal.

LUNES	MARTES	MIERCOLES	JUEVES	VIERNES	SABADO	DOMINGO
COMPLETA	COMPLETA	COMPLETA	COMPLETA	COMPLETA		