Introducción

Fondo Unido I.A.P se compromete a respetar tu privacidad y tus datos personales de acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("Ley"), su Reglamento, así como con la normativa y disposiciones análogas y complementarias en materia de protección de datos personales.

Por lo que hacemos de su conocimiento la infraestructura operativa y sistemas que nos permiten el tratamiento adecuado de los datos proporcionados a Fondo Unido I.A.P.

Auditorias

Fondo Unido I.A.P. realiza auditorías externas cada dos años con la finalidad de identificar y asegurar la mejora de puntos de seguridad, así como capacitación continua al personal activo de la organización. El proceso de selección de los auditores se define por un proceso de competencia y determinación de proveeduría por parte de los Comités de Administración y Finanzas. Así mismo se cuenta con el soporte técnico diario.

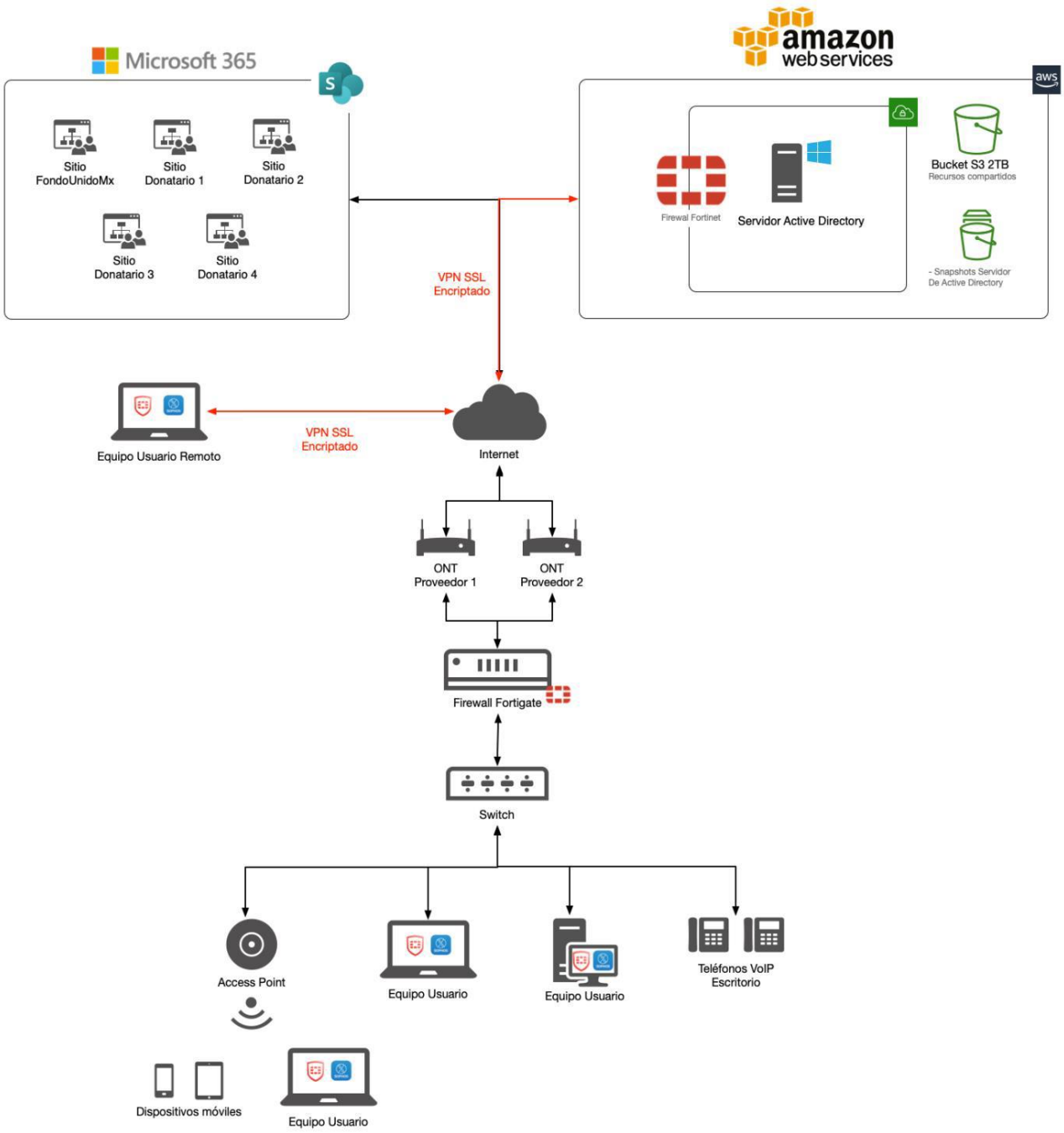
Auditoria IT: 2021
Diagnóstico de Sistema de Gestión y Seguridad de la Información: 2022

Infraestructura

Herramientas Institucionales que garantizan el cumplimiento de la seguridad:

- Dispositivos de protección y análisis de red en las instalaciones de la Fundación.
- Software de protección de última generación en equipos de cómputo.
- Dispositivos de protección y análisis de red en la nube de la Fundación.
- Directorio Activo en la nube, para el control y gestión de los equipos dentro y fuera de las instalaciones.
- Comunicaciones seguras a los recursos en la nube de la Fundación.
- Servicios de archivos compartidos en la nube.
- Sistema de respaldos por imagen del sistema.
- Servicios de archivos compartidos en SharePoint

Diagrama general de herramientas Fondo Unido I.A.P.



Río Pánuco núm. 15,
Col. Cuauhtémoc.
C.P. 06500, Ciudad de México.

fondounido.org.mx
+(52) 5566 3997
@FondoUnidoMx

Protección y análisis de red en las instalaciones de la Fundación

Fondo Unido I.A.P. cuenta con Firewall Fortinet el cual administra y analiza la red a través de las siguientes herramientas:

Separación de redes públicas y privadas

Privada: para usuarios propios de la Fundación, en la cual se encuentran accesibles recursos compartidos como las impresoras, telefonía IP, etc. la cual solo es accesible a través de los nodos de red cableada y a través de la red Wifi privada.
Pública: red para visitantes, proveedores y dispositivos de los usuarios de la fundación, que no requieran el acceso a ningún recurso. Esta red se encuentra limitada a los recursos de la fundación y solo cuenta con acceso a internet.

Firewall

El dispositivo tiene implementadas una serie de políticas sobre las redes LAN en las cuales no se permite ninguna solicitud de acceso a los dispositivos dentro de la red, lo que evita el acceso de usuarios malintencionados de fuera de la red a los recursos y equipos locales en la Fundación.

Protección Antivirus para el tráfico dentro de la red

Se tiene implementada el análisis del tráfico de los equipos dentro de la red y los archivos que se transmiten, esto con el fin de localizar y eliminar virus que intenten ser propagados de algún equipo de cómputo o algún dispositivo a otros dispositivos dentro de la red.

Esta tecnología analiza los archivos y los compara con firmas de virus reconocidos de las cuales se reciben actualizaciones varias veces al día.

Protección en la navegación web

EL firewall analiza todo el tráfico de los equipos dentro de la red ya sea cifrado o sin cifrar y de acuerdo con la clasificación y rating de las páginas web que los usuarios intentan visitar, bloquea el acceso a aquellas a que pueden estar categorizadas como peligrosas dentro de la base de datos de Fortinet.

Protección de acceso a contenido no permitido

Se cuenta con un filtrado de contenido para evitar que los usuarios puedan ingresar a páginas categorizadas como:

- Pornografía
- Drogas
- Citas
- Apuestas
- Odio y discriminación
- Armas
- Torturas
- Anonimizado de tráfico
- Desnudos
- Sexualidad

Redes Wifi Seguras

Se tiene implementado accesos Wifi que propagan la red privada y la red pública a través de las bandas de 2.4 GHz y 5 GHz, para aprovechar la mejor velocidad y también cuidar la compatibilidad. Estas redes están protegidas por contraseña y cifradas a través WPA2.

Protección de última generación en equipos de cómputo

Derivado de la pandemia de COVID-19 el esquema tradicional de trabajo ha cambiado y con ello los retos de protección a los usuarios, que ya no se encuentran en una sola ubicación y que además reciben muchas más amenazas las cuales los antivirus tradicionales no pueden contener.

Es por lo que se ha implementado una solución en seguridad llamada Sophos Intercept X Advanced en los equipos de cómputo de la Fundación. Este es compatible con sistemas operativos Windows y macOS .

Seguridad ante ransomware y virus

Intercept X es un software EDR (Endpoint Detection and Response), diseñado para la búsqueda de amenazas y protección de equipos a través del análisis de comportamiento y no por firmas de los archivos (como los antivirus tradicionales), esto hace que la amenaza sea mitigada desde el principio, ya que detecta e investiga la actividad sospechosa con un análisis basado en Inteligencia Artificial, y usa las siguientes herramientas para mejorar la protección:

- Detección de malware con Deep Learning
- Escaneado de archivos anti-malware
- Live Protection
- Análisis de comportamiento previo a la ejecución (HIPS)
- Bloqueo de aplicaciones no deseadas
- Sistema de prevención de intrusiones
- Análisis de comportamiento en tiempo de ejecución (HIPS)
- Interfaz de análisis antimalware (AMSI)
- Detección de tráfico malicioso (MTD)
- Prevención de exploits
- Mitigaciones de adversarios activos
- Protección contra archivos de ransomware (CryptoGuard)
- Protección del registro de arranque y disco (WipeGuard)
- Protección contra Man-in-the-Browser (Navegación segura)
- Bloqueo de aplicaciones mejorado

Protección de acceso a contenido no permitido

Cuenta con un filtrado de contenido a nivel equipo de cómputo y está configurado para evitar que los usuarios puedan ingresar a páginas categorizadas como:

- Pornografía
- Alcohol y tabaco
- Actividad Criminal
- Hacking
- Drogas ilegales
- Odio y discriminación
- Proxis
- Violencia
- Armas

Además de identificar a través de tipos de archivos y URL de origen, los archivos que pueden ser potencialmente peligrosos y bloquea su descarga.

Monitoreo de periféricos

Cuenta con herramientas de monitoreo y bloqueo de periféricos para que no se puedan utilizar unidades USB o discos duros externos no autorizados y evitar la extracción de información. De momento esta función se encuentra configurada en modo monitoreo y será habilitada posteriormente de acuerdo con el plan de mejoras.

Protección y análisis de red en la nube de Fondo Unido I.A.P.

Se cuenta con el servicio de Infrastructure as a Service (IaaS) en Amazon Web Services para el montado de recursos compartidos para los usuarios y de seguridad y control para los equipos de cómputo.
Esto se hace a través de una Virtual Private Cloud (VPC) que es una red privada virtual la cual está administrada y protegida por una instancia virtual FortiOS que cuenta con las siguientes herramientas de protección con las mismas características que su homólogo en las instalaciones de Fondo Unido I.A.P.:

- Firewall
- Protección Antivirus para el tráfico dentro de la red
- Salida a internet solo a servicios necesarios.

Comunicaciones seguras a los recursos de la Fundación

Para poder acceder a la nube o a la red local de Fondo Unido los usuarios tienen instalado en sus equipos de cómputo el programa llamado Forticlient, que funciona como cliente de VPN (Virtual Private Network) para poder acceder a los recursos de manera segura.

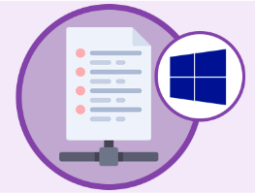
Este software realiza una conexión entre el equipo de cómputo que puede estar en cualquier parte del mundo y los Firewalls en la nube o las instalaciones de la Fundación a por un túnel con cifrado SSL a través de internet, con esto la información es protegida mientras viaja y no puede ser interceptada para su robo o alteración.

Directorio Activo en la nube

Para una mejor gestión y control de los equipos de cómputo y los usuarios, se ha implementado un servidor en la Nube el cual sirve como Controlador del Directorio Activo. implementado herramientas para la gestión de los equipos y mejoras de seguridad como son:

- Control de aplicaciones instaladas en los equipos.
- Prevención de modificación de opciones avanzadas del sistema.
- Uso de contraseñas seguras para el acceso a los equipos.
- Actualización de políticas de grupo.
- Privilegio mínimo a usuarios.

Servicios de archivos compartidos en la nube



Dentro del controlador de Directorio Activo, se ha implementado el servicio de archivos compartidos, esto para el uso con información interna de Fondo Unido I.A.P. y que no debe de ser accesible por terceros.

Para ello se utiliza un esquema de permisos documentados en una matriz de accesos la cual indica, el nivel de acceso (Sin acceso, Lectura, Lectura y escritura) que tiene un usuario con respecto a un determinado recurso compartido, y es controlado a través de grupos de acceso y pertenencia de usuarios a los mismos, garantizando la privacidad de la información.

Sistema de respaldos por imagen del sistema

Se cuenta con un sistema de respaldos por imagen (Snapshots) de los discos de sistema y almacenamiento de archivos.

Este tipo de respaldos realiza una copia idéntica del contenido de los discos duros, permitiendo recuperarlos al estado en que se encontraban en el momento que se generó la copia.
Esto es útil cuando los servidores tienen algún error o daño que evita que el sistema operativo arranque, ya que se pueden sustituir los discos dañados por uno con una configuración buena y recuperar toda la funcionalidad en un par de horas, a diferencia de recuperar de manera manual reinstalando y reconfigurando todos los servicios y programas.

También sirven como versionado de archivos en los recursos compartidos, para poder recuperar un archivo eliminado o una versión de un archivo en determinado momento.
La periodicidad y retención del sistema de respaldos es la siguiente:

- Respaldos diarios de los últimos 7 días (solo recursos compartidos)
- Respaldos semanales de las últimas 4 semanas
- Respaldos mensuales de los últimos 3 meses

Servicios de archivos compartidos en SharePoint

Actualmente se encuentra en uso la plataforma de Microsoft SharePoint como plataforma principal para compartir archivos internamente y con terceros.

Se implementaron las siguientes medidas para garantizar la privacidad, disponibilidad e integridad de la información:

- Sitio privados y limitados accesos a través de cuenta de Microsoft institucional.
- Implementación y control de permisos de acceso a través de una matriz de permisos para cada recurso compartido y cada usuario.
- Uso de versionados para recuperación en caso de borrado o modificación accidental.
- Sitio en internet para ser accesible desde cualquier lugar sin internet.

Destinatarios de Datos Personales y Finalidad

Destinatario de los datos personales	Finalidad
Área Contable	Gestión contable y fiscal
Proveedor de CFDI	Generación facturas electrónicas
Promotores y organizadores	Desarrollo de la campaña
Comunicación y Mercadotecnia	Comunicación, difusión de campañas y entrega de reportes cualitativos y cuantitativos de resultados a donantes.

Control de accesos

Fondo Unido cuenta con una matriz y proceso de acceso a los colaboradores a la información que sea requerida para la ejecución de sus actividades, con base a:

Nivel de Información:
. Restringido
. Confidencial
. Abierto

Accesos por perfil de colaborador:
. Sin acceso
. Lectura
. Colaborador (Editar)

Baja y cancelación de accesos

Durante el proceso de baja de un colaborador se realizan las siguientes actividades:

1. Aviso al área de Sistemas de la baja estipulando fecha.
2. Se realiza un respaldo en el equipo
3. Se reasigna o bien se da de baja el correo, con base al requerimiento de la Dirección correspondiente. En caso de reasignarse, en un periodo máximo de 3 meses se da de baja el correo.
4. Se realiza un cambio de contraseña del correo, en caso de reasignarse el mismo.
5. Se bloquean accesos al colaborador que se da de baja

Capacitación y actualización

Con base a las actualizaciones, recomendaciones y acciones implementadas en las auditorias, Fondo Unido realiza un plan de capacitación con los colaboradores y lo integra en el material de inducción.