Políticas DIGIFACT

Versión 1.9

INFORMACIÓN GENERAL

Control de cambios

Fecha	Versión	Autor	Revisado	Aprobado
01/05/2019	1.0	Asesor de Calidad	Gerente de Desarrollo	Ing. Francisco Palomo Gerente General

Revisiones

Fecha	Versión	Observaciones	Responsable
28/06/2019	1.1	Se modificó el apartado de la política de acceso lógico al Data Center en el apartado primero, se añadieron dos notas iniciales	Elías Avilés
2/07/2019	1.2	Se modificó el apartado de la política de manejo de la información en el numeral 10.1.4 añadiendo el apartado de Thawte RSA CA Se modificó el apartado 6.1.6 eliminando la palabra firma en todos los casos que se usa como referencia de llave	Elías Avilés
12/07/2019	1.3	Modificación del apartado 6.1.3 cambiando de posición algunos párrafos, agregando unas notas y robusteciendo el apartado final de la seguridad de las contraseñas obligando al cumplimiento de todas las recomendaciones en lugar de solamente 2 Modificación del apartado 6.1.4 agregando un apartado para incluir a SAT como un tercero que se conecta.	Elías Avilés
17/07/2019	1.4	Inclusión del apartado 6.3 y 6.3.1 relacionado a la política de seguridad de equipos personales Se actualizó la numeración del apartado 6.1.3 relacionado a las uso de contraseñas añadiendo los apartados 6.1.3.1.Seguridad de la Contraseña y 6.1.3.2. Prohibiciones en el manejo de contraseñas	Elías Avilés

Fecha	Versión	Observaciones	Responsable
25/07/2019	1.5	Cambio del apartado 4.1.4 de eliminación de bitácoras a retención de bitácoras, inclusión del apartado 4.1.5 monitoreo de bitácoras, 4.1.6 auditoría de bitácoras y 4.1.7 eliminación de bitácoras Se añadió numeración a los subtítulos correspondientes al apartado 10.1.12 quedando de la siguiente manera: 10.1.12.1 Digitalización de archivos 10.1.12.2 Respaldo de configuraciones 10.1.12.3 Respaldo de los registros de las bases de datos. En el apartado 10.1.12.2 se actualizo lo referente a los respaldos de las configuraciones en relación a FEL	Elías Avilés
26/07/2019	1.6	Se añadió todo lo referente al apartado 10.2 Política de gestión de riesgo	Elías Avilés
1/08/2019	1.7	Se cambió la redacción del apartado 10.2 eliminando la metodología de trabajo Se añadió el apartado 8.1 que hace referencia a la Política de análisis de vulnerabilidades el anterior apartado 8.1 y sus sub apartados se corrieron a la numeración 8.2	Elías Avilés
9/08/2019	1.8	Se realizó una reestructuración completa de la numeración eliminando lo relacionado introducción, objetivos, etc. De los distintos apartados. Se actualizó el índice según nueva estructura. Se añadieron los apartados relacionados a la actualización de seguridad 8 y aseguramiento de componentes9	Elías Avilés
7/7/2020	1.9	No tuvo cambios de fondo, solamente se actualizó logos.	María Álvarez

Índice

Controles de Acceso Lógico

1. Política de Acceso Lógico al Data Center

Nota 1: Derivado a que la infraestructura destinada a FEL, será en la nube, (AWS, Amazon Web Services).

Nota 2: El único acceso que se tendrá a dicha infraestructura será única y exclusivamente lógico.

Política: Cualquier persona que deba poseer credenciales de acceso lógico al Data Center deberá ser aprobada previamente por medio del registro "Solicitud de acceso a plataforma FEL e Infraestructura" el cual será validado por el Jefe superior inmediato para finalmente ser presentado a la gerencia de Soporte y Desarrollo quien dará la aprobación final para dar las credenciales de acceso.

Las autorizaciones de acceso lógico a los diferentes componentes que formen parte de la infraestructura FEL, deberán incluir principalmente, los equipos a los cuales podrá acceder, los niveles de privilegios que tendrá en cada equipo y el jefe inmediato del usuario.

La persona que deba tener acceso lógico a los servidores deberá de poseer un Identificador de Usuario único el cual le será asignado por parte del administrador de las credenciales de ingreso a los servidores. El administrador deberá crear el usuario dentro de la consola de administración de AWS asignando los niveles de privilegios necesarios acorde a las acciones que el usuario podrá realizar dentro de los equipos.

Los usuarios que deban tener acceso a las consolas del firewall virtual deberán solicitar al Administrador de la consola administrativa, la creación de su usuario haciendo entrega de la autorización respectiva con todos los datos necesarios. El Administrador de la Consola de AWS se encargará de crear el usuario para que puedan acceder a los diferentes Security Groups necesarios y otorgar las instrucciones de ingreso al usuario.

Los usuarios que deban tener acceso a las Bases de Datos de la infraestructura de servicio de la infraestructura FEL deberán solicitar al Administrador de la Consola AWS, que le provea los accesos necesarios para RDS, que es la lógica de base de datos que será utilizado para FEL.

Todos los accesos remotos hacia los servidores, equipos de red y Base de Datos (AWS RDS) dentro de la infraestructura de red del servicio de FEL, deberán ser realizados por medio de un método denominado bastión, este método de utilizar un host bastión es una solución que se utiliza con mucha frecuencia, con el propósito de proporcionar acceso a una red privada desde una red externa, como Internet. Debido a su exposición a un ataque potencial, un host de bastión debe minimizar las posibilidades de penetración.

Todos los usuarios que requieran un acceso remoto deberán utilizar el software otorgado por el administrador de la consola para la creación del túnel apropiado entre las diferentes VPN s la terminal que se desea conectar y el firewall. Esta será la única

forma en la que se encontrará permitido acceder remotamente a los equipos, cualquier otra forma de acceso será tomada como una violación a esta política.

Ninguno de los Administradores podrá, en ninguna circunstancia, crear un usuario sin recibir previamente la autorización escrita y firmada por la Dirección correspondiente. En caso un Administrador creara cuentas de usuario sin autorización, él será responsable de todo lo que pueda suceder a través de estas cuentas.

Todos los accesos lógicos hacia cualquier dispositivo deberán ser documentados por parte del dispositivo y/o algún agente externo el cual se encargará de mantener todos los datos de ingresos actualizados. Esta bitácora de registros deberá ser luego manejada según la Política de Manejo de Bitácoras.

1.1. Formato de Identificador de Usuario

Los nombres de usuario deberán ser creados bajo un formato estándar que deberá cumplir con los siguientes requerimientos:

- Deberá empezar con la letra inicial del primer nombre del usuario que se está registrando.
- Luego de la primera letra deberá ir el primer apellido completo del usuario.

Ej. La creación del usuario Juan Pérez indicaría que el Identificador de usuario será jperez.

En caso el nombre de usuario ya existiera, se deberán de tomar la cantidad de letras que sean necesarias del segundo nombre para crear un Identificador de Usuario que aún no se encuentre en uso (se iniciará tomando la primera letra del segundo nombre y se podrá tomar el nombre completo si fuera necesario).

Gestión de bitácoras

2. Política de Manejo de Bitácoras

Política: Todas las bitácoras deberán ser almacenadas a través del sistema de gestión de bitácoras propio del sistema.

Todos los equipos de hardware y aplicaciones de software que se encuentren prestando un servicio, deberán contar con bitácoras automáticas, generada, a nivel de equipo interno, todo tipo de transacción estará almacenada dentro del EVENT_VIEWER de cada equipo.
De tal manera que, en ambiente de producción, los servidores involucrados almacenarán información, de acuerdo a su rol en la infraestructura FEL.
Respecto a la plataforma como tal y las diferentes operaciones que cada EFACE realice, se estarán almacenando dentro de una de la base de datos dentro de la instancia en RDS destinado para dicho efecto.

Por tanto, todo tipo de LOG estará verificándose en dos modalidades, que es la modalidad de infraestructura, y la modalidad de plataforma en sí.
Para las bitácoras a nivel de infraestructura se estarán manejando, las herramientas de 1CloudWatch y DashBoard de Sophos.
Para las bitácoras a nivel de plataforma FEL, se estará manejando tanto EventViewer dentro de cada sistema operativo, como a nivel de base de datos FactLog, alojado en la instancia dentro de RDS.

2.1. Bitácoras de Instancias de Infraestructura

En el caso de la lógica en la NUBE, cada instancia maneja su respectivo dashboard (CloudWatch), dentro de dicho dashboard, se monitoreará el rendimiento de cada equipo.
CloudWatch, maneja una serie de alarmas por default, las mismas se estarán monitoreando diariamente.

2.2. Bitácora de Plataforma FEL

Las Bitácoras de aplicaciones, o bien de la plataforma FEL, como tal estarán tanto en el EventViewer y cualquier transacción se encontrará en la base de datos FactLog dentro de la instancia alojada en AWS RDS.

Las mismas serán extraídas si y solo si, son solicitadas explícitamente al departamento de Informática.

2.3. Bitácoras de Bases de Datos

El Sistema de Gestión de Bases de Datos, se hará por medio de AWS RDS.

Todas las Bases de Datos que se encuentren corriendo dentro del Sistema de Gestión de Bases de Datos se encontrarán ligadas al procedimiento de SNAPSHOTS, que maneja AWS RDS.
Las bases de datos como tal contendrán información transaccional importante de cada uno de nuestros EFACE's, almacenando información encriptada con un algoritmo especial dentro de la plataforma, y otros en BASE64.

2.4. Retención de Bitácoras

La retención de la información transaccional de la plataforma se encontrará almacenada en bases de datos, las cuales se retendrán en un periodo de 1 a 2 años, de acuerdo con la documentación que rige la nueva modalidad de Factura Electrónica en Línea (FEL).
FEL, establece que la retención mínima de la información es de Un (1) año, por lo que nuestra plataforma retendrá como mínimo Un (1) año, a un máximo Dos (2) años.

La información de periodos anteriores podrá encontrarse en la instancia de base de datos actual, o bien podrá encontrarse en el Bucket correspondiente, en formato (.BAK).

2.5. Monitoreo de Bitácoras

Toda transacción que se realice en la plataforma FEL, quedará almacenada en el visor de eventos, que WINDOWS tiene de forma nativa.

Cada capa de la arquitectura, FRONT y BACK, contarán con el visor de eventos catalogado como digifact.com.fact.

En el visor de eventos digifact.com.fact, se mostrarán todas las transacciones tanto en Warning, Error o Información.

2.6. Auditoria de Bitácoras

Con la ayuda de las herramientas del visor de eventos de Windows, y de la base de datos FactLog, se podrá monitorear y auditar, cualquier transacción. De igual manera se podrá verificar algunos detalles de éstas, tales como:

1. Tipo de Transacción
2. País de Origen
3. Entidad emisora de la transacción
4. Fecha y hora en que se dio la transacción
5. Mensaje descriptivo del problema en WARNING o ERROR

Ejemplo de evento en ERROR:

Transaction=AUTHENTICATE_USER
Country=GT
Entity=JQFWOFJO
UserName=GT.JQFWOFJO.BPlABonc
<Dictionary name="IssuerTaxIdBadFormat">
<Entry k="EventName" v="NitDelEmisor"/>
<Entry k="EventId" v="3123"/>
<Entry k="EventToken" v="SENDER_NIT_BAD_FORMAT"/>
<Entry k="Processor" v="WIN-HAGRA3IPKN8"/>
<Entry k="Module" v="mx.com.fact.util.dll"/>
<Entry k="Class" v="TransactionTag"/>
<Entry k="Method" v="PreValidateEntity"/>
<Entry k="TimeStamp" v="2019-06-20T00:21:46"/>
<Entry k="Description" v="El NIT del emisor (ó Entity) no tiene el formato correcto."/>
<Entry k="Hint" v="Favor de corregir según las reglas del país de emisión."/>
<Entry k="Message" v="Entity=JQFWOFJO"/>
</Dictionary>

En la base de datos FactLog, se almacenará toda transacción, adicional a ello contendrá la IP origen de la transacción, siendo un dato relevante para trasladar al FIREWALL SOPHOS, si fuera necesario, o bien contactar a la entidad generadora, para indicarle el problema que la plataforma ha detectado de las diferentes solicitudes realizadas.

2.7. Eliminación de Bitácoras

Todas las bitácoras que sean eliminadas, ya sea dentro de EC2, como dentro de RDS o del lugar de almacenamiento definitivo, deberá seguir el procedimiento de eliminación de bitácoras, debiendo llenar toda la documentación necesaria sin afectar la operación de FEL como tal.

Seguridad de la Información

3. Políticas y Normas de Seguridad Informática

Política: Todos los usuarios de la infraestructura FEL deberán observar todas y cada una de las políticas de Seguridad Informática para evitar cualquier tipo de ataque en contra la infraestructura misma, así como cualquier tipo de fuga de información que pudiera suscitarse debido a ellos. La seguridad Informática deberá observarse y cuidarse. Al encontrarse la infraestructura en la NUBE AWS, nos permite realizar actualizaciones eficientemente sin comprometer el servicio de FEL como tal.

3.1. Actualización o migración de SERVIDOR

Las actualizaciones o migraciones de las instancias EC2, se deberán hacer de acuerdo al procedimiento creado para dicho fin, refiérase a **Procedimiento de Migración**.
Siendo nuestros sistemas operativos WINDOWS, sabemos que es de alguna manera recomendable migrar a una versión más reciente.

3.2. Accesos externos a la infraestructura, Controles de Código Malicioso (Firewall SOPHOS), Equipo de usuarios colaboradores.

Para evitar cualquier ataque informático por medio de cualquier tipo de código malicioso, el personal de Cyber Espacio, S.A. podrá usar únicamente el acceso mediante el bastión, o por medio del firewall.

Los usuarios deben cuidar que la información que manejan y los medios de almacenamiento autorizados para uso dentro de la empresa se mantengan libres de cualquier tipo de amenaza por código malicioso, esto deberán hacerlo a través del software antivirus instalado dentro de sus computadoras.

Ningún usuario interno o externo podrá descargar software con cualquier origen, sin el debido análisis y autorización previa por parte del Departamento de Informática.

Los usuarios no pueden alterar o eliminar cualquier tipo de configuración del software antivirus instalado en su máquina, incluyendo la desinstalación del mismo. Cualquier cambio que se deba realizar a estas configuraciones deberá ser analizado, aprobado y realizado única y exclusivamente por personal del Departamento de Informática.

La forma en la que trabaja el código malicioso es muy compleja y sofisticada, generando cambios en las configuraciones más importantes del equipo, por lo que se prohíbe que cualquier usuario intente erradicar los ataques de este tipo por sí mismo, ya que puede agravar el problema.

3.3. Uso de Contraseñas

Cada usuario de los equipos dentro de la red deberá contar con un Identificador de Usuario único dentro de la infraestructura FEL, el cual le servirá para acceder a los equipos que sean necesarios. El usuario será el único responsable de cualquier acción realizada desde su usuario, por lo que el usuario deberá cuidar la confidencialidad de su Identificador de Usuario y su Contraseña.

Las contraseñas serán cambiadas cada 6 meses. Por ende, cuando las contraseñas caduquen deberán ser remplazadas con una nueva contraseña que cumpla con todas las reglas de seguridad, por lo que se debe estar atentos a solicitarla, y tenerla lista.

Es obligación del usuario cambiar la clave por defecto asignada a su cuenta por el departamento de Informática, cuidando que la nueva contraseña cuente con las medidas de seguridad recomendadas.

3.3.1. Seguridad de la Contraseña

Al crear una contraseña el usuario deberá tomar en cuenta las siguientes reglas de creación de contraseñas para asegurar al máximo sus contraseñas:

- Crear contraseñas de al menos ocho caracteres: Mientras más larga sea la contraseña, mejor.
- Mezclar letras mayúsculas y minúsculas: Utilice esta mezcla de caracteres para tener una contraseña más segura.
- Mezclar letras y números: Agregar números a las contraseñas, especialmente cuando se añaden en el medio (no solamente al comienzo o al final), puede mejorar la fortaleza de la contraseña.
- Incluya caracteres no alfanuméricos: Los caracteres especiales tales como &, $ y # pueden mejorar considerablemente las contraseñas.
- Seleccione una contraseña que pueda recordar: Seleccione una contraseña que cumpla con las reglas de seguridad, pero que pueda recordar de manera fácil.

Las contraseñas que cree el usuario deberán cumplir todas las recomendaciones anteriores para cumplir con la seguridad solicitada por la organización.

Nota 1: Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá solicitar al departamento de Informática que se realice el proceso respectivo para la recuperación de la contraseña (véase Proceso de Recuperación de Contraseña).

Nota 2: Cuando se tenga la sospecha que personas no autorizadas han tenido acceso a su contraseña de usuario, la misma se deberá sustituir inmediatamente por una nueva que cumpla con las reglas de seguridad recomendadas y que sea completamente diferente de la contraseña actual.

3.3.2. Prohibiciones en el manejo de contraseñas

- Se prohíbe cualquier tipo de ayuda escrita o impresa referente a la contraseña en lugares donde personas no autorizadas puedan descubrirlos.

- Compartir las contraseñas con terceros queda terminantemente prohibido. La persona que comparta la contraseña será totalmente responsable de todo lo que se haga con la misma.

- Queda prohibido que el usuario almacene su contraseña en cualquier programa que otorgue esta facilidad.

3.3.3. Conexiones Externas

La infraestructura AWS Amazon, cuenta con una forma de acceso que es efectivamente externa. El acceso a los componentes de la infraestructura solo podrá hacerse por medio del bastión, o firewall.

En cuanto a los diferentes EFACE's, la única forma de conexión será por medio https, bajo el certificado de seguridad emitido por la entidad THWATE, ESSET, ya sea por medio de API Rest, o WebService ASMX.

Respecto a la conexión con SAT se ha expuesto de igual manera un API Rest que se encuentra expuesto bajo el mismo protocolo seguro https:// felgtaws.digifact.com.gt/felrtu/api/rtu

3.3.4. Seguridad Perimetral

La infraestructura de FEL, cuenta con la solución de SOHOS, esta cumple con todas las condiciones de seguridad perimetral o IPS.

3.3.5. Manejo de Llaves de Encriptación Firma CERTIFICADOR

La nueva modalidad de Factura Electrónica FEL, garantiza el manejo de la llave electrónica compartida por la entidad aceptada para generar firmas avanzadas. Para el caso de DIGIFACT la entidad es la Cámara de Comercio.

La llave tiene uso exclusivo para FEL.

La llave se resguardará, en el módulo que AWS Amazon FIPS 140-2 LEVEL 2.
Dentro del servicio Key Managment Service o (KMS).

La renovación de la llave se hará con un periodo de 2 meses de antelación previo a su fecha de vencimiento.

La instalación de la actualización de la llave la deberá hacer el/la Gerente de Desarrollo.
.

4. Políticas del Firewall SOPHOS

El firewall deberá manejar una política de denegación, bloqueando todos los puertos que no se encuentren abiertos por medio de instrucciones específicas.

Todos los puertos que se encuentren abiertos deberán tener una razón plenamente justificada para encontrarse en este estado y estas razones deberán encontrarse documentadas para un mejor control de la infraestructura de seguridad en la red.

4.1. Utilización del Internet

El acceso a Internet otorgado dentro de las instalaciones de Cyber Espacio, S.A. para el personal deberá ser utilizado única y exclusivamente para el desarrollo de las actividades relacionadas con todo lo concerniente a aplicaciones informáticas.

Todos los accesos a Internet que sean necesarios dentro de las instalaciones de Cyber Espacio, S.A. deberán ser realizados por las vías provistas por el departamento de Informática de la organización. Cualquier otra forma de enlace que sea necesaria deberá ser solicitada y autorizada por el departamento de Informática.

Los usuarios de Internet que sospechen de algún incidente deberán reportarlo inmediatamente al departamento de Informática, junto con la justificación de sus sospechas. El caso deberá de contar con el seguimiento respectivo por parte del departamento de Informática.

Todos los usuarios del servicio de Internet, junto con la aceptación del servicio aceptan las siguientes condiciones:

- Toda actividad realizada se encontrará sujeta a monitoreo.
- Se encuentra prohibido el acceso a páginas no autorizadas (véase documento de páginas no autorizadas).
- Se prohíbe la descarga de cualquier tipo de archivo sin la autorización previa del departamento de Informática.
- La utilización del Internet de la organización es para el desempeño de sus diversas funciones dentro de la empresa, el uso del servicio con propósitos personales queda prohibido.
- Se prohíbe la transmisión de datos confidenciales o reservados utilizando el servicio de Internet, no importa la forma en la que se transporten los datos.

4.2. Violaciones de Seguridad Informática

Se prohíbe el uso de cualquier tipo de herramienta (hardware, software, etc.) a través de la cual se violen los controles de seguridad informática. El uso de estas herramientas quedará autorizado única y exclusivamente al personal del departamento de Informática, en ambientes controlados y con previa autorización de la dirección del departamento.
Se prohíbe a cualquier usuario ajeno al departamento de Informática realizar pruebas a los controles de seguridad de la organización, ninguna persona debe probar o intentar comprometer los controles internos a menos que cuente con la aprobación de la dirección del departamento de Informática y se realice en un ambiente de pruebas controlado.
Cualquier persona que de manera intencional escriba, genere, compile, coleccione, propague, ejecute o intente introducir cualquier tipo de código (programa) utilizado para ataques informáticos (virus, gusanos, caballos de Troya, etc.) diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes, servicios o información de Cyber Espacio, S.A., será reportado con las autoridades correspondientes quienes deberán darle seguimiento al caso y aplicar las sanciones correspondientes.

5. Política de Seguridad de Equipos Personales

Todo equipo debe tener habilitada la sección de **Cifrado de unidad BitLocker** en las plantillas administrativas del sistema operativo Windows, dentro de los componentes de Windows.

Se permite únicamente los siguientes dispositivos:

- Equipo PC y/o MAC (Portátil o Desktop.)
- Discos Duros externos previamente revisados y escaneados.

Se determina como como equipos o dispositivos no permitidos los siguientes:

- Unidades extraíbles (USB's)
- Dispositivos Móviles (Android, IOS u otro similares).

5.1. Firewall en los equipos

Respecto al Firewall, todo equipo deberá encontrarse debidamente activado y con todas las reglas INBOUND/OUTBOUND, debidamente configuradas.

Gestión de vulnerabilidades

6. Política de análisis de vulnerabilidades

Política: Se estarán realizando evaluaciones y remediaciones de vulnerabilidades reales y potenciales al menos trimestralmente, así como también luego de la realización de cambios significativos en el sistema. Este análisis será realizado por el personal asignado por la Gerencia de Desarrollo bajo la supervisión del Gerente.

7. Política de Actualización de Componentes por Medio de Parches.

Política: La plataforma FEL desarrollada por Cyber Espacio Digifact utiliza la última versión de la AMI oficial de Windows Server. Al momento de realizar una actualización de los componentes se deberá crear la Golden image, para luego proceder a la instalación de los últimos parches y finalmente realizar la configuración de los paquetes y aplicaciones.
La actividad de actualización de los componentes por medio de parches estará directamente bajo la responsabilidad del encargado de infraestructura y deberá realizarse al menos una vez cada mes.

8. Política de Aseguramiento de Componentes

Política: El aseguramiento de los componentes dentro de los servicios de la nube será garantizado por medio de la creación de la imagen y actualización de la plantilla de AWS CloudFormation. Luego se deberá actualizar la pila de información dentro del CloudFormation y finalmente realizar el reemplazo de los servidores activos de manera individual.

Esta actividad deberá ser realizada bajo la responsabilidad del encargado de infraestructura y deberá realizarse al menos una vez cada mes.

9. Política de Control de Cambios

Política: Cualquier tipo de cambio que deba ser realizado dentro de la infraestructura FEL, deberá ser documentada y presentada a la comisión de Control de Cambios, la cual deberá analizar la propuesta junto con sus beneficios y posibles consecuencias para la toma de una decisión respecto a la realización del cambio. En caso la respuesta fuera positiva se deberá calendarizar el cambio para el inicio de las pruebas respectivas (en caso no hayan sido realizadas) para la posterior implantación del cambio.

9.1. Comité de Control de Cambios

El comité de Control de Cambios deberá estar conformado por al menos un representante financiero, auditoría y uno del área técnica. Los cambios que deban ser realizados en la infraestructura del servicio FEL deberá ser analizado en estos tres campos para saber de qué manera pueden afectar tanto en costos, cumplimiento de normativa y cambios a nivel de plataforma o software.

Los cambios que se propongan deberán ser entregados junto con una explicación detallada del cambio que se desea realizar, los antecedentes que justifican el cambio, así como los posibles beneficios y problemas que puede presentar en cada una de las áreas representadas en el comité (financiero, auditoria y técnico). En base a estos datos entregados, el comité deberá realizar el análisis respectivo y entregar una respuesta a los solicitantes del cambio.

Cualquier miembro o grupo de miembros de la organización podrá realizar una propuesta de cambio, siempre y cuando éste se encuentre plenamente justificado y sea un cambio factible. La propuesta de cambio podrá ser revisada por cualquiera de los integrantes del comité de cambios de manera individual, pudiendo ser descartada luego de la negativa de al menos dos de los miembros.

Luego de presentada una propuesta de cambio, el comité tendrá un máximo de 7 días calendario para presentar una resolución respecto al cambio, la respuesta deberá quedar documentada sea esta positiva o negativa, así como las razones de la decisión.

9.2. Propuestas de Cambios

Todas las propuestas de cambios que se deseen realizar deberán ser analizadas inicialmente por el departamento que crea conveniente el cambio, las propuestas serán entregadas y serán responsabilidad del departamento que la presente.

Las propuestas deberán contener toda la información detallada del cambio, las implicaciones del cambio, los análisis realizados para las diversas áreas representadas en el comité (si aplica) incluyendo también los resultados de las series de pruebas realizadas respecto a la implementación del cambio. También deberá describir la forma de implementación del cambio.

9.3. Implementación de cambios

Todos los cambios que sean autorizados por el Comité de Cambios deberá ser previamente calendarizado de manera inmediata por el o los departamentos responsables de la aplicación del cambio.

Antes de la aplicación del cambio, se deberán realizar pruebas exhaustivas en ambientes de prueba creados especialmente para esto. Ningún cambio podrá ser realizado si no existe una serie de pruebas que demuestre que el mismo no significará riesgo alguno en la infraestructura y/o plataforma FEL en su ambiente de producción.

Cuando un cambio haya completado la serie de pruebas respectiva podrá ser aplicado en el ambiente de producción. La implementación deberá ser realizada en horarios no hábiles o de poca afluencia transaccional (De 12:00 AM a 4:00 AM) para afectar en menor medida los servicios expuestos de la plataforma.

Cualquier ventana de mantenimiento generada debido a la implementación de un cambio deberá ser informada vía correo electrónico a todos los EFACE's que se puedan ver afectados por algún tipo de corte en el servicio. El correo deberá contener los detalles del cambio a realizar, así como las fechas y horarios de la ventana y también la duración de esta.
No se podrá efectuar ninguna implementación sin antes haber enviado las notificaciones respectivas a los clientes.

Antes de la implementación de un cambio, se deberá crear un respaldo de las configuraciones que se afectarán, esto para tener un punto de restauración (ROLLBACK) previo al cambio, en caso éste se tuviera que revertir. En caso el cambio no fuera efectivo, se deberán deshacer todas las configuraciones realizadas y aplicar el respaldo que se obtuvo antes del cambio.

Los encargados de la realización de las ventanas de mantenimiento se encuentran también encargados de que al momento de la finalización de la ventana el servicio o los servicios se encuentren trabajando en óptimas condiciones. No se podrán realizar ventanas de mantenimiento que dejen el servicio funcionando de manera ineficiente o incorrecta.

9.4. Mantenimientos

Todos los mantenimientos de equipos y/o software que sea necesario deberán ser realizados de acuerdo a los manuales de procesos y procedimientos correspondientes. Los mantenimientos deberán ser realizados única y exclusivamente por los encargados de estos procesos para evitar poner en riesgo los servicios en línea.

Todos los mantenimientos deberán ser realizados con autorización previa de la Dirección respectiva y el Departamento de Informática para evitar interrumpir las labores del departamento.

Todos los mantenimientos en las áreas críticas de la infraestructura y que puedan afectar los servicios en línea de la organización deberán ser realizados dentro de una ventana de mantenimiento que será programada en horarios de bajo nivel transaccional (12:00 AM a 4:00 AM) de los servicios y se deberá informar a todos los clientes acerca de los datos generales del mantenimiento y de las posibles implicaciones en el servicio prestado.

Los mantenimientos de emergencia serán realizados en cualquier horario que sea requerido, buscando siempre resolver el problema en el menor tiempo posible e incluso utilizando soluciones temporales. La prioridad de un mantenimiento de emergencia siempre será el de restablecer el servicio en la mayoría de su capacidad, o en una capacidad suficiente para mantener a los clientes que necesiten encontrarse en línea en esos momentos.

Todos los mantenimientos deberán documentarse indicando el objeto del mantenimiento, las acciones realizadas, los estados del objeto antes y después del mantenimiento y todos los datos consignados en el procedimiento de mantenimiento respectivo.

Los mantenimientos deberán ser realizados de manera que los servicios queden de funcionales luego de la aplicación del mantenimiento, en caso contrario se deberá revertir cualquier cambio en configuraciones que haya sido realizado durante el mantenimiento.

Cualquier cambio de configuraciones que sea programado deberá iniciar con la realización de un respaldo de las configuraciones de los programas que se modificarán. En caso el mantenimiento no fuera exitoso en el ambiente de producción, todos los datos dentro del respaldo de configuraciones deberán ser restaurados de manera inmediata y buscar nuevas opciones para realizar el mantenimiento que se aplicaba.

10. Política de Manejo de la Información

Política: Toda la información que sea manejada dentro de la organización deberá ser catalogada y dividida en secciones que especifiquen el tipo de información que se está manejando. Cada tipo de información deberá tener un encargado quién velará por el nivel de seguridad que le otorgará a cada tipo de información que maneje. El encargado de la información es el principal responsable del correcto manejo de la misma y de las personas y/o entidades que podrán tener acceso a esta información.

Toda la información deberá ser manejada de acuerdo al nivel de protección otorgado a la misma, de esta manera, la información confidencial deberá ser almacenada tomando en cuenta siempre la confidencialidad, integridad y disponibilidad de la misma.
La misma será accedida únicamente por el encargado de la información y las personas que sean autorizadas, tomando la responsabilidad de estas autorizaciones, el

encargado asignado. Todo acceso a información confidencial deberá quedar documentado para constancia en cualquier momento que se necesite.

De tal manera que la plataforma FEL, deberá proporcionarle al administrador de la información de cada EFACE, un usuario y contraseña que le permita visualizar su información siempre.
De igual manera le permitirá al administrador, crear, otorgar y/o denegar permisos a otros que así considere conveniente.

Toda la información que sea de poca importancia podrá ser manejada de manera más simple y el encargado de la información podrá dar acceso a la misma sin necesidad de ningún tipo de documentación alterna. De igual manera la información que deba ser pública deberá ser publicada en lugares dónde todo el personal de la organización lo pueda ver y leer.

10.1. Propiedad de la Información

Toda persona que sea responsable de un tipo o forma de información será considerado el propietario de la misma. Como el propietario de la información tendrá la obligación y responsabilidad de cuidar el acceso a la misma dependiendo del tipo de información manejada. El propietario de la información deberá también clasificar la información según la forma en la que se deba manejar, indicando si la información es confidencial, privada, simple o pública.

El propietario de la información será el único que tenga acceso a la misma, a menos que el mismo propietario autorice a otra persona para tener acceso. Esta autorización deberá quedar documentada indicando a qué información tendrá acceso la otra persona y la razón por la cual requiere este acceso. Esto aplicará para la información que sea considerada de tipo confidencial o privado.

10.2. Tipos de Información

La información dentro de la organización será manejada en cuatro rangos de importancia los cuales se explican a continuación:

- Información Confidencial: Esta información podrá ser manejada única y exclusivamente por el dueño de la misma. Cualquier tipo de acceso por parte de otra persona deberá ser autorizado previamente por el dueño de la información quien estará encargado de documentar la autorización indicando la fecha y razón del acceso, así como la información que fue accesada. Esta información debe ser almacenada cumpliendo las características de Confidencialidad, Integridad y Disponibilidad de la Información.

- Información Privada: Esta información podrá ser manejada única y exclusivamente por el dueño de la misma. Cualquier tipo de acceso por parte de otra persona deberá ser autorizado previamente por el dueño de la información, este acceso podrá quedar documentado de manera opcional.

Cualquier mal uso de la información accesada podrá ser imputado al dueño de la información, por lo que se deberá cuidar a las personas que tienen acceso.

- Información simple: Se trata de cualquier información que pueda encontrarse dentro de la organización y que no contiene ningún dato que pueda ser utilizado de manera perjudicial. El dueño de esta información podrá compartirla con las personas que crea pertinente sin necesidad de ningún tipo de documentación, pero siempre será responsable de todo lo que pueda suceder por este acceso.

- Información pública: Esta información debe ser accedida y conocida por cualquier persona dentro de la organización, por lo que el dueño de la misma se encontrará encargado de facilitar los accesos a la información colocándola en lugares públicos y de fácil acceso.

Cualquier información generada en los diversos departamentos de la organización deberá ser clasificada dentro de alguno de los tipos de información mencionados anteriormente y se deberá asignar la propiedad de los mismos.

10.3. Formas de la Información

La información podrá existir de únicamente de manera lógica. Será considerada información física cuando se encuentre en un documento impreso en papel o algún material que pueda ser palpado de manera física. La información lógica será la que se encuentre almacenada dentro de las bases de datos o en documentos de cualquier tipo y extensión (como PDF, XML, CSV, XLSX, etc), así como los registros de cualquier forma de información que se encuentre almacenada en medios como Discos Duros, CDs, DVDs, medios extraíbles y todo medio de almacenamiento magnético u óptico.

La información física que requiera de seguridad especial (confidencial) deberá ser resguardada a través de medios físicos efectivos (armarios con candados, etc.) que aseguren el acceso a la información única y exclusivamente por el propietario de la información y las personas que él autorice.

La información virtual que requiera de seguridad especial (confidencial) deberá ser resguardada a través de medios lógicos (firewall, encriptaciones, accesos lógicos, etc.) que aseguren el acceso a la información única y exclusivamente por el propietario de la información y las personas que él autorice.

10.4. Encriptación de Comunicaciones

Todas las comunicaciones que se realicen entre entes externos y la organización deberán realizarse a través de medios seguros para la distribución de la información, específicamente cuando se desea intercambiar información confidencial.

Los servicios prestados y que deban manejar información confidencial serán encriptados utilizando protocolos seguros para la transmisión de los datos a través de la red. Ninguna comunicación que contenga información confidencial podrá ser realizada por los medios convencionales de transmisión de datos con el fin de evitar

cualquier acceso no autorizado a la información, actualmente los sitios a los que accede serán única y exclusivamente https.

Para tal efecto se cuenta con el servicio de Thawte RSA CA, que es el ente que extiende el certificado de los medios seguros para la distribución de información. La parte de encriptación se detalla en el "**procedimiento de encriptación de conexiones**".

10.5. Uso del Correo Electrónico

Los usuarios no deben usar cuentas de correo electrónico pertenecientes a otras personas ni recibir mensajes en cuentas de alguien más. En caso fuera necesario que alguien leyera el correo de otra persona que se encuentra fuera o de vacaciones, la persona ausente deberá direccionar el correo hacia la cuenta de correo interno de la otra persona. Queda prohibido direccionar los correos a una cuenta de correo que sea externa a Cyber Espacio, S.A., a menos que se cuente con la autorización del Departamento de Informática.

Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos recibidos en las cuentas de la organización o que contengan información de la organización, como información propiedad de Cyber Espacio, S.A. Los mensajes siempre deben ser una comunicación privada entre emisor y receptor.

Los usuarios podrán enviar información reservada y/o confidencial a través de correo electrónico, pero esta deberá ir encriptada y destinada exclusivamente a personas autorizadas que se encuentren en el ejercicio estricto de sus funciones y atribuciones.

Cyber Espacio, S.A. podrá analizar y acceder a todos los mensajes y archivos adjuntos enviados a través del correo institucional si existiera algún tipo de sospecha plenamente justificada de que se ha enviado información que puede comprometer la red o de cualquier otra acción no autorizada.

El usuario utilizará el correo electrónico exclusivamente para desempeñar las tareas que le fueron asignadas dentro de la organización por su cargo, empleo o comisión; cualquier otra forma de uso del correo electrónico se encuentra prohibida.

Queda terminantemente prohibido suplantar, falsear o suprimir la identidad de un usuario del correo electrónico. El único caso válido para borrar una cuenta de correo electrónico es siguiendo el proceso de separación del cargo de alguno de los miembros de la organización.

Queda prohibido interceptar o revelar las comunicaciones por correo electrónico de la empresa, al igual que la ayuda a terceros para realizar cualquiera de estas acciones. De igual manera queda prohibido cualquier intento (aunque fuera fallido) de realizar las acciones descritas anteriormente, ya que éste será tomado y tratado de igual manera que un ataque concretado.

10.6. Administración de Privilegios

Cualquier cambio en la infraestructura organizacional que implique el cambio de rol de una persona, y por ende un cambio en los privilegios de acceso a la información, deberá ser notificado al área de Informática por medio de solicitud enviada por el Gerente del área que necesita el cambio o la autoridad que lo ordena.

10.7. Confidencialidad y Privacidad

Todos los empleados deberán firmar un contrato de confidencialidad con la empresa antes de iniciar las relaciones laborales, esto con el fin de asegurar que toda la información a la cual tendrá acceso será conservada en completa confidencialidad.

Los empleados deberán tener acceso a la información y equipos que su puesto y/o responsabilidades requieran, siempre con la autorización de los dueños de la información y los encargados de los equipos.

Los empleados deberán cuidar sus datos personales y de acceso a los diversos sistemas a los que tenga acceso, ya que cualquier tipo de acción realizada a través de sus credenciales de usuario será responsabilidad total y completa del empleado dueño de las credenciales.

10.8. Equipo desatendido

El usuario que deja su lugar de trabajo por alguna razón, deberá bloquear el equipo con el que se encuentra trabajando. El bloqueo se deberá realizar a través del control de acceso lógico asignado al equipo en uso.

10.9. Periféricos y Dispositivos Especiales

Los usuarios del área de Informática que deban manejar físicamente los servidores por cualquier actividad asignada, podrán usar los periféricos y dispositivos especiales únicamente previa autorización de autoridad superior (Jefe de Informática) y luego de una exhaustiva revisión de los mismos. Todos los periféricos a usar deberán pasar por una revisión de archivos realizada por la persona designada y luego por un análisis antivirus exhaustivo.

El uso indebido de estos dispositivos será responsabilidad total del usuario que realice los cambios en el equipo, lo cual será comprobado a través de los logs de los servidores y luego de un análisis forense de los mismos.

10.10. Documentación del Sistema

Todos los sistemas de los servicios que sean prestados de manera interna y/o externa a la organización deberán ser documentados de manera completa, contando como

mínimo con manuales técnicos y de usuario de cada uno de los módulos del sistema. De los proyectos desarrollados dentro de la empresa se solicitará la documentación de seguimiento y desarrollo del proyecto, dependiendo el tipo de proyecto desarrollado.

Toda la documentación del sistema deberá ser almacenada en un lugar centralizado, buscando cumplir con las características de Confidencialidad, Integridad y Disponibilidad de la información. La información de los manuales deberá ser publicada en lugares dónde cualquier usuario pueda tener acceso a la misma, asegurando que ninguno tenga problemas al momento de utilizar alguno de los servicios prestados por la organización.

Cuando varias personas deban tener acceso a la misma información y todas deban tener la capacidad de modificarla al mismo tiempo (desarrollos de proyectos de software especialmente), deberán utilizar un servicio de versionado de documentos y algún servidor de repositorio que ayude a controlar la información por diversas personas y cuidando las características esenciales de la misma.

10.11. Derechos de Propiedad Intelectual

Se prohíbe la reproducción total o parcial de programas de ordenador o cualquier otro software sin la autorización escrita del autor, ya sea este adquirido o desarrollado por Cyber Espacio, S.A. (interna o externamente).

Los sistemas desarrollados por personal interno o externo bajo la supervisión del Departamento de Informática son propiedad intelectual de Cyber Espacio, S.A.

10.12. Respaldo de la Información

Toda la información confidencial que sea crítica para la organización deberá de contar con un respaldo el cual deberá ser realizado de acuerdo al procedimiento respectivo dependiendo del tipo de información respaldada. Entre este tipo de información se encuentran los archivos de configuraciones de los Sistemas Operativos, Equipos críticos de la red (firewall, switches), Bases de Datos así como también el respaldo de todas las bitácoras de los equipos incluyendo pero no limitándose a las de los Sistemas Operativos de los servidores, equipos de red (firewall, switches), Base de Datos, Sistemas de Control de Acceso tanto físico como lógico.

10.12.1. Digitalización de archivos

Todos los documentos físicos que necesiten tener un respaldo deberán ser digitalizados a través de una copia digital del mismo en formato pdf. Luego estos archivos deberán ser centralizados en un equipo de almacenamiento temporal dónde permanecerán al menos un mes.

Todos los archivos que sean digitalizados deberán ser nombrados acorde a lo que contienen, debiendo contener al menos una referencia al departamento al cual

pertenece el documento, la persona del departamento que solicitó la digitalización, la persona que lo digitalizó, la fecha de digitalización y un nombre para el archivo. En caso el archivo no se pueda nombrar con las características anteriormente descritas, se deberá adjuntar un archivo de texto plano que contenga esta información y toda la que se considere pertinente.

Cualquier tipo de información física podrá ser digitalizada, únicamente se deberá seguir el procedimiento respectivo para la digitalización de la información llenando la documentación respectiva y dejando constancia de los pasos realizados para lograr obtener la copia digitalizada. Dependiendo del tipo de información que se está digitalizando así será la seguridad con la que se deberá digitalizar y manejar luego el archivo digital.

El personal encargado de digitalizar no podrá conocer el tipo de información que se encuentra digitalizando y le queda terminantemente prohibido ingresar a consultar la información que acaba de digitalizar.

10.12.2. Respaldo de Configuraciones

Se deberá de realizar un respaldo de todos los archivos de configuraciones de los equipos que se encuentren prestando servicios de alta disponibilidad, especialmente los dedicados al servicio de Generación de Facturas Electrónicas.

Las configuraciones que se deben respaldar serán las de las Aplicaciones que corren prestando el servicio, los Sistemas Operativos de los equipos (servidores, firewall, switches), de las Bases de Datos y sus Sistemas de Administración respectivos.

Todos los archivos de configuraciones que sean respaldados deberán ser probados luego de su extracción para comprobar que son funcionales, estas pruebas se podrán hacer en un ambiente de pruebas o se podrán realizar simples inspecciones visuales luego de la extracción para corroborar el éxito de la operación. Cualquier tipo de error presentado durante la generación del respaldo obligará a la creación de un nuevo respaldo para asegurar el éxito de la operación.

La plataforma FEL, que se encuentra bajo la infraestructura AWS de AMAZON, cuenta con la ventaja de ser auto escalable. Los diferentes componentes que se encuentran involucrados en la plataforma FEL así también como su respectiva configuración y los diferentes scripts necesarios para dar de alta cualquier componente en cualquier momento.

Tomando en cuenta que la herramienta S3 que Amazon ofrece, se agregará un bucket cross region, es decir en una región diferente a la región donde se encuentra el sitio FEL. Dentro del bucket, se encontrarán los recursos necesarios, scripts de componentes y todo lo necesario.

El almacenamiento de los recursos en el bucket cross región, hará que sea un medio alterno de almacenamiento, que cuenta con una disponibilidad del 99.99%, así también cumple con el aspecto de confidencialidad e integridad. La información contenida en dicha carpeta, únicamente debe ser modificada, cada vez que la

plataforma FEL, necesite algún tipo de modificación o upgrade, garantizando que la información y la configuración siempre sea una última versión vigente.

Semestralmente se deberá escoger el último respaldo almacenado y un respaldo al azar que haya sido generado con menos de un año de antigüedad, estos deberán ser probados en un ambiente de pruebas para comprobar su integridad y su utilidad ante cualquier tipo de incidente.

Los respaldos que se harán de las configuraciones deberán ser completos, tomando todos los archivos necesarios para la configuración que se está respaldando.

Se encuentra terminantemente prohibido la alteración de cualquiera de las configuraciones de los equipos, establecer redes de área local, conexiones remotas internas o externas, el intercambio de información a través de cualquier protocolo de transferencia de datos (FTP, SSH, etc.). Este tipo de eventos serán permitidos única y exclusivamente previa autorización del Departamento de Informática.

10.12.3. Respaldo de los registros en las Bases de Datos

Se deberá realizar como mínimo un respaldo diario de los registros de la Base de Datos del servicio de Generación de Facturas electrónicas. Este respaldo deberá ser almacenado en un equipo de almacenamiento temporal que se encontrará dentro de la red de la Base de Datos.

Al iniciar el proceso de respaldos de los registros de la Base de Datos se deberá realizar un respaldo completo de la misma, luego de esto se generarán respaldos diarios del tipo diferencial. Semanalmente se generará un respaldo completo de los registros en la Base de Datos.

Mensualmente se deberán tomar los últimos dos respaldos completos del mes junto con la última semana de respaldos diferenciales y deberán ser copiados en uno o varios CDs o DVDs (dependiendo del tamaño del respaldo) para su posterior transporte hacia el sitio de almacenamiento definitivo.

Todos los respaldos que se realicen de los registros de las Bases de Datos deberán ser realizados durante horas no hábiles del servicio (madrugadas) y se deberán realizar por medio de un procedimiento almacenado que se encontrará siendo ejecutado de manera automática dentro del Sistema de Administración de Bases de Datos en los horarios y días respectivos.

Semestralmente se deberán realizar pruebas de restauración con el último respaldo completo utilizado junto con el último backup diferencial para comprobar la integridad y utilidad de los datos respaldados.

Los respaldos de las Bases de Datos deberán ser conservados durante por lo menos 5 años después de la fecha de su generación. Con esta política se cumplirá la exigencia de la SAT de conservar los documentos generados durante por lo menos 5 años.

10.12.4. Respaldo de Bitácoras

Todo el manejo del respaldo de las diversas bitácoras existentes en el sistema se encuentra indicado en la "Política de Manejo de Bitácoras".

10.13. Resguardo y Protección de la Información

Todos los usuarios deberán reportar de forma inmediata al Área de Informática cuando detecte que existen riesgos reales o potenciales que presente el área física en que desempeñan sus funciones para los equipos de cómputo o de comunicación de los que hacen uso. Estos riesgos pueden ser ambientales (fugas de agua, conatos de incendio, etc.) o de seguridad (archivos expuestos, falta o facilidad de contraseñas, etc.)

Todos los medios de almacenamiento de información de tipo extraíble asignados por Cyber Espacio, S.A. a un usuario en función de sus tareas dentro de la empresa, son su responsabilidad, al igual que toda la información que este medio contenga aunque estos no se utilicen.

Toda la información que se encuentre dentro de las computadoras asignadas a los trabajadores de Cyber Espacio, S.A. será su responsabilidad, al igual que evitar cualquier tipo de fuga o pérdida de información dentro de los equipos.

Toda la información que sea generada derivado de los servicios que presta la organización deberán ser respaldados por copias de seguridad diaria, los cuales serán almacenados en un lugar seguro, cuidando siempre la Confidencialidad, Disponibilidad e Integridad de la Información.

Todos los respaldos de información que sean generados en CD o DVD de manera mensual deberán ser transportados hacia el lugar de almacenamiento definitivo que deberá de encontrarse en un lugar remoto a la ubicación del Data Center que resguarda los equipos que prestan el servicio. El traslado deberá ser realizado de manera confidencial en días y horarios diferentes a los cuales únicamente tendrá acceso el jefe de la logística de traslados del Departamento de Informática.

10.14. Baja o eliminación de Equipos

Toda baja de Equipos que se encuentren involucrados, en el procedimiento FEL, que por alguna razón deba ser retirado de la infraestructura de la nube AWS. Deberá hacerlos previo análisis del departamento de informático, garantizando que no exista perdida alguna de información que pueda afectar el buen funcionamiento de la plataforma FEL como tal.

11. Política de gestión de riesgo

Debido a la importancia que tiene la detección pronta de riesgos que sean amenazas para los activos críticos FEL se estará realizando un análisis de riesgos al menos una vez al año a todos los activos relacionados con la operación FEL., Esta operación será realizada por personal de Desarrollo con la supervisión de la Gerencia de Desarrollo.

Sanciones por incumplimiento de políticas

Sanciones de las Autoridades.

Económicas y administrativas que emitan las entidades regulatorias, al no cumplir con los requerimientos y especificaciones establecidos para adquisición, mantenimiento y control de la infraestructura de Tecnología de Información.

Personal de la empresa

De no cumplirse con las políticas por parte del área de Sistemas, deben aplicar las siguientes sanciones:
1a. Falta: Amonestación verbal.
2a. Falta: Acta administrativa.
3a. Falta: Despido por incumplimiento.