CPA CONTROL DE COMPROBANTES DIGITALES S. DE R. L. DE C.V.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Fecha de la versión:	*03/10/2018*
Creado por:	*Jefe de Operaciones*
Revisado por:	*Gerente de Operaciones XPD*
Aprobado por:	*Gerente General de Operaciones*

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/04/2017	1.0	Saúl Huerta Cortés	Elaboración del documento.
03/10/2017	2.0	José Luis Lozada Hernández	Revisión del documento y actualización
03/04/2018	3.0	Jefe de Desarrollo	Revisión, actualización de "historial de modificaciones", integración de política "Respaldo de información local" y modificación de diagrama de comité de seguridad de la Información.
03/10/2018	4.0	Jefe de Operaciones	Actualización en los puestos que autorizan el documento, modificación de diagrama de comité de seguridad de la información.

Creado por:	Revisado por:	Aprobado por:
Jefe de Operaciones	Gerente de Operaciones XPD	Gerente General de Operaciones

CONTENIDO

1 Objetivo

El propósito de este documento de Políticas de Seguridad de la Información es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Los usuarios de este documento son todos los empleados de CPA CONTROL DE COMPROBANTES DIGITALES (en adelante XPD), como también terceros y externos a la organización.

2 Alcance

En XPD se entiende que la Seguridad de la Información es la preservación, protección y resguardo de los activos de información contra una amplia gama de amenazas para asegurar su confidencialidad, disponibilidad e integridad, de manera tal que se asegure la continuidad de las operaciones y minimizar el daño sobre los clientes, en primera instancia, y en la organización.

Por tal motivo, la Dirección de XPD reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, bases de conocimiento, manuales, casos de estudio, códigos fuente, estrategia, gestión, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente las políticas plasmadas en este documento.

Garantizar que la información permanece confidencial sin perder su integridad y disponibilidad para cumplir con la normatividad vigente.

La seguridad de la información se caracteriza por la preservación de:

a) Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.

b) Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.

c) Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto de controles, tales como políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles han sido establecidos para asegurar que se cumplen los objetivos específicos de seguridad de la empresa.

Las políticas presentadas en este documento son de aplicación obligatoria para todo el personal de XPD, así como a cualquier tercero que participe en el uso, aplicación, explotación y mantenimiento de las tecnologías de información propiedad de la empresa.

De la misma manera, este documento ampara todos servicios prestados por XPD, que están respaldados por las certificaciones como Proveedor de Certificación de Comprobantes Digitales por Internet (PCCFDI), Proveedor de Certificados para la Expedición de CFDI a través del Adquiriente de Bienes o Servicios (PCECFDI), Proveedor de Certificación de Recepción de Documentos Digitales (PCRDD) y Proveedor de Servicios de Certificación (PSC), sobre las cuales se realiza el cumplimiento legal y normativo, que también se refleja en lo definido en estas políticas.

3 Compromiso de la Dirección

La Dirección General de XPD aprueba la Política de la Organización en Seguridad de la Información y su Políticas Específicas de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas que garanticen la seguridad de la información en la empresa.

La Alta Dirección de XPD demuestra su compromiso a través de:

- La revisión y aprobación de las Política de la Organización en Seguridad de la Información y su Políticas Específicas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este documento a todos los empleados, proveedores y terceros de la organización.

- El aseguramiento de los recursos para implementar y mantener la Política de la Organización en Seguridad de la Información y su Políticas Específicas de Seguridad de la Información.

- La verificación del cumplimiento de las políticas aquí mencionadas.

- Facilitar la existencia de un plan de difusión de la Política de la Organización en Seguridad de la Información y su Políticas Específicas de Seguridad de la Información.

Propiciar la existencia de mecanismos o procedimientos que aseguren la continuidad del negocio ante situaciones que impidan el acceso a la información imprescindible para el funcionamiento de la organización.

3.1 Publicación y Difusión de las Políticas

Para asegurar que la Política de la Organización en la Seguridad de la Información y las Políticas Específicas de Seguridad de la Información se integran en la cultura organizacional de XPD, se establece la existencia de un Plan de Difusión, Capacitación y Sensibilización en torno a la seguridad de la información, que aplica para el personal interno y externo de la organización.

El Responsable de la Seguridad de la Información debe asegurar la existencia permanente y el cumplimiento del Plan de Difusión, Capacitación y Sensibilización de la seguridad de la información.

Las versiones vigentes de Política de la Organización en Seguridad de la Información y su Políticas Específicas de Seguridad de la Información, así como la documentación vinculada a la seguridad de información son publicadas en el repositorio oficial de XPD.

3.2 Revisión de las Políticas

La presente Política de la Organización en la Seguridad de la Información y las Políticas Específicas de Seguridad de la Información que de ésta se derivan y que se encuentran contenidas en este documento, son revisadas cada 6 meses o cuando XPD lo requiera para asegurar la continuidad de la organización, considerando los cambios que puedan producirse, tales como: enfoques a la gestión de seguridad, circunstancias de la compañía, cambios legales, cambios al

ambiente técnico, recomendaciones realizadas por autoridades pertinentes, tendencias relacionadas con amenazas y las vulnerabilidades, entre otras.

Cada modificación sobre el presente documento debe estar registrada en el apartado de control de cambios, así como en la Lista Maestra de Documentos

4 Introducción a las Políticas de Seguridad de la Información

En XPD la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones, razón por la cual existe un compromiso expreso de protección de sus propiedades como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, XPD implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las políticas de seguridad de la información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en XPD; este proceso es liderado de manera permanente por el Responsable de Seguridad de la Información.

5 Objetivos de Seguridad de la Empresa

5.1 Objetivo General

Asegurar la integridad, confidencialidad y disponibilidad para toda la información en XPD, para mantener la continuidad operacional de los procesos y servicios de la organización, mediante el resguardo de los activos de información de los procesos del negocio y su soporte.

5.2 Objetivos Específicos

- Identificar, clasificar y asignar los dueños de los activos de información para lograr niveles esperados de integridad, confidencialidad y disponibilidad de éstos.
- Controlar, prevenir y/o mitigar los riesgos de seguridad de la información, identificando las vulnerabilidades y amenazas sobre los activos, para asegurar la continuidad del negocio.
- Establecer políticas y procedimientos que permitan resguardar y proteger los activos de información de XPD.
- Definir, ejecutar y controlar un Plan de Difusión, Sensibilización y Capacitación que permita difundir a todo el personal de XPD los alcances y buenas prácticas asociadas a la seguridad de la información, establecidas dentro de la organización.

6 Política de la Organización en la Seguridad de la Información

XPD ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la empresa en cuanto a la protección de sus activos de Información:

1. Existe un Comité de Seguridad de la Información que es el responsable del mantenimiento, revisión y mejora de las políticas y procedimientos de seguridad de la Información de XPD.

2. Los activos de información de XPD son identificados y clasificados para establecer los mecanismos de protección necesarios.

3. XPD define e implanta controles para proteger la información contra violaciones de autenticidad, accesos no autorizados y la pérdida de integridad para garantizar la disponibilidad requerida por los clientes y usuarios de los servicios, ofrecidos por la empresa.

4. Todos los empleados, subcontratados y/o proveedores son responsables de proteger la información a la cual acceden y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5. Se realizan auditorías y controles periódicos sobre las políticas y procedimientos de seguridad de la información de XPD, de acuerdo al Plan de Auditoría de la organización.

6. Es responsabilidad de todos los empleados reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

7. Es responsabilidad de todos los subcontratados y/o proveedores solicitar el registro de incidentes de seguridad a empleados de XPD, cuando sean identificados por éstos.

8. Las violaciones a las políticas y controles de seguridad de la información son reportadas, registradas y monitoreadas, a través de la herramienta de gestión de servicio y clasificadas como incidentes de seguridad.

9. XPD cuenta con un Plan de Continuidad del Negocio que asegura la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

La Política de la Organización en Seguridad de la Información y su Políticas Específicas de Seguridad de la Información establecidas en XPD, así como sus procedimientos se encuentran alineados a las mejores prácticas internacionales como: ISO 27001, ISO 9001, ISO 22301, ISO 27005 e ISO 20000.

7 Políticas Específicas de Seguridad de la Información

7.1 Política de Acuerdos de Confidencialidad

Todos los empleados de XPD y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la empresa, los cuales reflejan los compromisos de protección y buen uso de la información. Todos los acuerdos de confidencialidad no tienen vigencia, esto con el fin de mantener la seguridad sobre la información, aun cuando los empleados o terceros hayan dejado de colaborar con la organización.

Para el caso de contratistas o proveedores, los respectivos contratos deben incluir una cláusula de confidencialidad, cuando se permita el acceso a la información y/o a los recursos de XPD a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

7.2 Política de Intercambio de Información

XPD firma acuerdos de confidencialidad con los empleados, clientes y terceros que por diferentes razones requieren conocer o intercambiar información restringida o confidencial de la empresa. En estos acuerdos quedan especificados las responsabilidades para el intercambio de la información para cada una de las partes y se deben firmar antes de permitir el acceso o uso de dicha información.

Todo empleado de XPD es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma, y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad.

7.3 Política de Clasificación de la Información

Toda la información de XPD debe ser identificada, clasificada y documentada, considerando el Procedimiento de Etiquetado y Manejo de la Información para preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte del personal interno, externo y proveedores que se encuentren autorizados y requieran de ella para la ejecución de sus actividades.

Para clasificar un activo de información se evalúan las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

a) Confidencialidad:

Nivel	Descripción
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la organización o no: PÚBLICO.
1	Información que puede ser conocida y utilizada por todos los empleados y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados puede ocasionar riesgos o pérdidas leves para XPD o terceros: RESERVADA – USO INTERNO.
2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados puede ocasionar pérdidas significativas a la organización o a terceros: RESERVADA – CONFIDENCIAL.
3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la Alta Dirección de la organización, y cuya divulgación o uso no autorizados puede ocasionar pérdidas graves al mismo a terceros. RESERVADA – SECRETA.

b) Integridad:

Nivel	Descripción
0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación de la organización.
1	Información cuya modificación no autorizada puede repararse aunque puede ocasionar pérdidas leves para la organización o terceros.
2	Información cuya modificación no autorizada es de difícil reparación y puede ocasionar pérdidas significativas para la organización o terceros.
3	Información cuya modificación no autorizada no puede repararse, ocasionando pérdidas a la organización o a terceros.

c) Disponibilidad:

Nivel	Descripción
0	Información cuya inaccesibilidad no afecta la operación de la organización.
1	Información cuya inaccesibilidad permanente durante 48 horas puede ocasionar pérdidas significativas para la organización o terceros.
2	Información cuya inaccesibilidad permanente 24 horas puede ocasionar pérdidas significativas para la organización o terceros.
3	Información cuya inaccesibilidad permanente durante 12 horas puede ocasionar pérdidas significativas para la organización o terceros.

Al referirse a pérdidas, se contemplan aquellas medibles (materiales) y no medibles (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asigna a la información un valor por cada uno de estos criterios. Luego, se clasifica la información en una de las siguientes categorías, según la tabla:

Clasificación de la Información				
	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3
Confidencialidad				
Integridad				
Disponibilidad				

Criticidad Baja: ninguno de los valores asignados supera el 1.	**Criticidad Media:** alguno de los valores asignados es 2	**Criticidad Alta:** alguno de los valores asignados es 3 en adelante

Sólo el Propietario de la Información puede asignar o cambiar el nivel de clasificación, cumpliendo con los siguientes requisitos previos:

• Asignarle una fecha de entrada en vigor.

• Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el Propietario de la misma identifica los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deben tener acceso a la misma.

En adelante se menciona como “información clasificada” o “datos clasificados” a aquella que se encuadre en los niveles 1, 2 o 3 de confidencialidad.

7.4 Política de Etiquetado y Manejo de la Información

XPD cuenta con un Procedimiento para el Etiquetado y Manejo de Información de acuerdo al esquema de clasificación definido. Los mismos contemplan los recursos de información tanto en formatos físicos como electrónicos.

Todos los activos de información deben tener identificado un Propietario o Responsable, ya sea a través del cargo o rol, y su clasificación basada en el nivel de resguardo que debe tenerse con relación a la integridad, disponibilidad y confidencialidad de estos activos y según la matriz de clasificación definida en la Política de Clasificación de la Información.

El Propietario de la Información es el responsable del etiquetado de la información, misma que debe realizar independiente al medio físico de manejo. Las actividades que requieran acceso a la información solo pueden ser realizadas por colaboradores autorizados por el Responsable de Seguridad de la Información, a menos que el Propietario así lo autorice, para casos puntuales.

A las reuniones donde se trate información confidencial, solamente pueden asistir las personas que hayan sido previamente invitadas, las que en todo caso deben ser validadas por el Propietario. Si se divulga oralmente información confidencial en una reunión, el expositor debe indicar la clasificación de la información, exigir discreción y eliminar cualquier información usada en la reunión.

El copiado o reproducción de los activos de información sean estos independientes del medio (papel, electrónico, etc.) deben aplicar las mismas

políticas y normas de seguridad definidas para los activos de información originales.

7.5 Política para Seguridad de los Recursos Humanos

Como parte de los términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación, deben entregar una Carta de No Antecedentes Penales y firmar un Acuerdo de Confidencialidad, en lo que respecta al tratamiento de la información de XPD. La copia firmada de dicho acuerdo es retenida por el área de Recursos Humanos. Así mismo, mediante el Acuerdo de Confidencialidad el empleado declara conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo, y en el entendido de que dicha confidencialidad se extiende más allá de la organización.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de propiedad intelectual o la legislación de protección de datos, se encuentran aclarados e incluidos en los términos y condiciones de empleo.

Todos los empleados reciben una capacitación y actualización en materia de la política, normas y procedimientos de XPD. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso de las instalaciones de procesamiento de información y el uso de los recursos en general, como por ejemplo su estación de trabajo.

El área de Seguridad de la Información es la encargada de coordinar las acciones de capacitación que surjan de la presente política.

De manera semestral, el Responsable de Seguridad de la Información y el Responsable de Capacitación del área de Recursos Humanos revisan el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización.

Las siguientes áreas son las encargadas de producir y proporcionar evidencia para el material de capacitación de seguridad de la información: departamento de Desarrollo y Operación y el área de Seguridad de la Información de XPD.

El personal que ingresa recibe el material y se le indica el comportamiento esperado en lo que respecta a la seguridad de la información, antes de que le sean otorgados los privilegios de acceso a los sistemas que corresponda.

7.6 Política de Riesgos relacionados con Terceros

El departamento de Desarrollo y Operaciones en conjunto con el área responsable de la Seguridad de la Información de XPD, identifican los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Los controles que se establecen a partir del análisis de riesgos, mismo que contempla riesgos internos y externo, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

7.7 Política de Uso de Contraseñas

Todos los recursos de información XPD tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada empleado requiere para el desarrollo de sus funciones, definidos y aprobados por el Jefe inmediato y administrados por el Jefe de Desarrollo y el Jefe de Operaciones.

Todo empleado o tercero que requiera tener acceso a los sistemas de información de XPD debe estar debidamente autorizado por el Propietario de la Información, para acceder a dichos sistemas haciendo uso de un usuario (ID) y una contraseña (password) asignados por la organización. El empleado debe ser responsable por el buen uso de las credenciales de acceso asignadas.
Las reglas para la generación de contraseñas a los recursos informáticos son:

1. La contraseña debe tener un mínimo de 8 caracteres.
2. La contraseña para las cuentas privilegiadas deben tener un mínimo de 8 caracteres.

Las contraseñas deben cumplir con al menos 3 de las siguientes características:

3. Debe tener al menos una letra en mayúscula.
4. Debe tener al menos una letra en minúscula.
5. Debe tener al menos un carácter numérico.

6. Debe contener al menos un carácter especial, como pueden ser: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

La contraseña debe permanecer cifrada en el aplicativo que se utilice, siempre que el sistema la permita. En el caso de los aplicativos, una vez que el usuario inicie sesión por primera vez, ninguna característica del aplicativo debe estar disponible hasta que el usuario no defina una contraseña que tome en cuenta los puntos anteriormente mencionados.

Todos los empleados o terceros que cuenten con accesos a los recursos informáticos deben apegarse a lo siguiente:

1. No escribir sus contraseñas en papeles de fácil acceso.
2. Las contraseñas se deben mantener confidenciales en todo momento.
3. No compartir las contraseñas con otros usuarios.
4. Si se sospecha que una contraseña ha sido compartida, ésta se debe cambiar en todos los sistemas a los que el usuario tiene acceso.
5. Las contraseñas se cambian cada 6 meses.
6. Para las cuentas privilegiadas las contraseñas se cambian cada 3 meses.

7.8 Política de Equipo Desatendido

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los empleados de XPD deben mantener la información confidencial o secreta bajo llave, cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información que se envía a las impresoras sea recogida de manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados, siempre que sea posible.

Todas las estaciones de trabajo deben usar el papel tapiz y el protector de pantalla corporativo, el cual se activa automáticamente después de 5 minutos de inactividad y se puede desbloquear únicamente con la contraseña del usuario.

El Responsable de Seguridad de la Información puede realizar revisiones sin previo aviso para asegurarse del cumplimiento de esta política, apegándose a las sanciones definidas en el apartado Medidas Disciplinarias por Incumplimiento a las Políticas.

Por cumplimiento a la Matriz de Controles (SAT) no aplica esta política para personal externo.

7.9 Política de Escritorio y Pantalla Limpia

Los equipos de escritorio y portátiles de XPD deben tener aplicado el protector de pantalla, mismo que se activa después de 5 minutos sin uso, siempre que el empleado se mantenga en su lugar, ya que de lo contrario debe bloquear su sesión durante su ausencia para proteger el acceso a las aplicaciones y servicios de la organización.

La pantalla de autenticación a la red de XPD debe requerir solo la identificación de la cuenta y la contraseña, sin mostrar ningún otro tipo de información.

Cuando el empleado deba ausentarse de su estación de trabajo, o bien finalice su jornada laboral debe guardar en un lugar seguro cualquier documento, medio magnético o removible que contenga información confidencial o de uso interno.

Además, previo a finalizar su jornada laboral el empleado debe desconectarse en su totalidad de computadoras centrales y servidores, evitando solo apagar el monitor o dejar en modo hibernación el equipo de cómputo, siempre que sea posible.

Si el empleado está ubicado en zonas de atención al público debe guardar los documentos e información en lugares seguros.

Los equipos de reproducción de información, tales como fotocopiadoras, impresoras o escáneres deben ubicarse en lugares de acceso controlado y cualquier documento con información confidencial o secreta debe retirarse inmediatamente de dicho equipo.

El empleado debe asegurarse en todo momento de no tener nombre de usuario y/o contraseñas apuntados en papel y dispuestos en lugares visibles.

El Responsable de Seguridad de la Información puede realizar revisiones sin previo aviso para asegurarse del cumplimiento de esta política, apegándose a las sanciones definidas en el apartado de Medidas Disciplinarias por Incumplimiento a las Políticas.

7.10 Política de Eliminación de Derechos de Acceso

El Jefe inmediato debe notificar cualquier desvinculación a la Dirección Operaciones de XPD, al área de Recursos Humanos y al área de Sistemas. Una vez realizada la notificación el Jefe inmediato debe gestionar la recuperación de los activos asignados al empleado, tales como:

- Documentos corporativos
- Equipo de cómputo
- Dispositivos de almacenamiento
- Software asignado
- Teléfono fijo
- Manuales

Cuando el empleado es desvinculado de la compañía, el área de Recursos Humanos realiza la notificación de baja, mediante correo electrónico, a la Gerencia de Operaciones XPD, departamento de Operaciones y Desarrollo, Jefe inmediato, Responsable de Seguridad de la Información y al Asesor de Tecnología Informática.

Una vez que recibido el correo de notificación, el Jefe inmediato solicita al Asesor de Tecnología Informática y a los Jefes de Desarrollo y Operaciones, realizar la eliminación de los derechos de acceso a los sistemas de información. El Jefe inmediato retiene el equipo para su asignación posterior.

7.11 Política de Gestión de Activos

XPD como propietario de la información física así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, tiene responsabilidad sobre cada uno de sus activos de información.

Toda la información de la organización, así como los activos donde ésta se almacena y se procesa, se asigna a un responsable de acuerdo con los criterios establecidos en la Política de Uso Aceptable de Activos, Política de Devolución de Activos, Política de Manejo y Etiquetado de Información así como la Política de Clasificación de la Información, que se mencionan en este documento.

7.11.1 Política para la Adquisición de Activos

Todo hardware y software debe ser adquirido conforme al Procedimiento de Compras de XPD y de acuerdo a los estándares de compatibilidad de sistemas de la compañía.

La compra de hardware, software y servicios para XPD deben ser comprados, rentados, prestados u obtenidos de un vendedor que pueda proveer servicios de mantenimiento, así como garantías.

7.11.2 Política para el Inventario de Activos

El Jefe de Desarrollo y el Jefe de Operaciones en conjunto con el Asesor de Tecnología Informática deben preparar un inventario de sistemas de información, detallando todo lo existente en hardware y software, tales como: bases de datos, routers, firewall y antivirus.

El Responsable de Seguridad de la Información debe mantener el control del inventario de activos, asegurándose de la actualización continua, de acuerdo a los movimientos que sufran cada uno de éstos.

7.11.3 Contenido del Inventario de Activos

Cada activo registrado en el Inventario de Activos debe incluir la siguiente información:

- Descripción del Activo
- Tipo de Activo
- Código del Activo
- Marca
- Modelo

- Serie
- Versión
- IP (en servidores)
- MAC Address (en equipos locales)
- Ubicación Física/ Lógica
- Propietario del Activo
- Custodio del Activo
- Dueño del Activo
- Clasificación del Activo
- Nivel de Protección del Activo

7.12 Política de Devolución de Activos

El empleado es responsable de devolver todos los activos que le fueron asignados al inicio y durante su relación laboral con la organización, como consecuencia de la finalización de su contrato y conforme a lo establecido en los Acuerdos de Confidencialidad.

Si el empleado posee información confidencial o secreta para la operación de XPD, es su responsabilidad entregar dicha información y transferirla al área correspondiente.

En caso de que el empleado haya hecho uso de equipos personales, es responsabilidad de éste transferir toda la información pertinente y eliminarla de su equipo, tomando en consideración lo establecido en la Política de Copias de Respaldo.

7.13 Política de Uso Aceptable de los Activos

El acceso a los documentos físicos y digitales está determinado por la Política de Clasificación de la Información, mencionada en este documento.

Para la consulta de documentos cargados en el software de gestión documental de XPD, se han establecido privilegios de acceso para los empleados y/o proveedores, de acuerdo con el desarrollo de sus funciones y competencias.

Dichos privilegios son establecidos por la Gerencia de Operaciones XPD, el Jefe de Desarrollo y/o el Jefe de Operaciones, quien comunica al Asesor de Tecnología Informática el listado con los empleados y sus privilegios.

Todos los empleados y terceros que manipulen información en el desarrollo de sus funciones deben firmar un "Acuerdo de Confidencialidad de la Información" donde se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este párrafo será considerada como un "incidente de seguridad".

7.14 Política para la Gestión de Incidentes de Seguridad de la Información y Gestión de Problemas

Los incidentes relativos a la seguridad deben ser comunicados tan pronto como sea posible por los empleados de XPD, a través del Procedimiento de Gestión de Incidentes establecido en la organización.

En caso de que el incidente sea detectado por un tercero, éste deberá comunicarlo a algún empleado de XPD para que sea posible comenzar con el tratamiento definido.

El Responsable de Seguridad de la Información, el Jefe de Desarrollo y el Jefe de Operaciones deberán valorar los eventos de seguridad de información y decidir si han de ser clasificados como incidentes de seguridad de la información.

De igual manera, el Responsable de Seguridad de la Información, en conjunto con el Jefe de Desarrollo y el Jefe de Operaciones, tienen la responsabilidad de organizar y mantener un equipo para la atención de incidentes de seguridad. Este equipo tiene el compromiso de dar seguimiento y brindar una respuesta ante la situación.

Los incidentes de seguridad, igual que los incidentes de operación, deben ser documentados para crear una base de datos de conocimiento. Los conocimientos adquiridos a partir del análisis y la resolución de incidentes de seguridad de información se deben utilizar para reducir la probabilidad o el impacto de los incidentes en el futuro.

La información recopilada en cada una de las etapas de la resolución de incidentes de seguridad sirve como evidencia que debe ser resguardada para posibles auditorías.

El Responsable de Seguridad de la Información debe asegurarse de notificar a las autoridades que correspondan, según sea el caso, acerca del incidente y su resolución, siguiendo lo establecido en el Procedimiento para el Contacto y Comunicación con las autoridades.

Los incidentes de seguridad de la información deben ser revisados bajo la Gestión de Problemas, definida en XPD, con el fin de llevar a cabo un análisis de causa raíz que permita encontrar la razón por la cual se generó la situación, así como establecer un plan de mitigación del problema y recomendaciones de mejora.

El análisis de causa raíz debe ser documentado en la base de datos de conocimiento de la compañía.

El Responsable de Seguridad de la Información debe dar seguimiento a los incidentes y problemas de información, además de apoyar en la facilitación de la resolución de incidentes y los planes de mitigación y mejora de problemas.

XPD mantiene contacto con grupo especialistas en seguridad de la información de los cuales obtiene conocimiento que puede ser aplicado en la resolución de incidentes o cualquier otra situación referente al tema.

7.15 Política de Control de Acceso Físico

Todas las áreas destinadas al procesamiento o almacenamiento de información así como aquellas en las que se encuentran los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro, que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan demostrar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), para garantizar que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

La Gerencia de Operaciones XPD y la el departamento de Operaciones y Desarrollo de XPD son responsables de otorgar los accesos al personal que así considere, a las áreas restringidas.

7.16 Política de Protección y Ubicación de los Equipos

Los equipos que son parte de la infraestructura tecnológica de XPD tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información, deben ser ubicados y protegidos para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se deben adoptar controles para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los empleados y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de XPD no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

El departamento de Operaciones y Desarrollo de XPD asegura las condiciones ambientales de las zonas donde se encuentran los equipos.

7.17 Política de Control de Acceso Lógico

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de XPD debe ser asignado de acuerdo a las políticas establecidas por la organización, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica de XPD asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos de autorización, los cuales deben ser revisados de manera periódica por el Responsable de Seguridad de la Información de XPD.
La autorización para el acceso a los sistemas de información debe ser definida y aprobada por el área propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los empleados y terceros.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de XPD, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autorizado por el Responsable de Seguridad de la Información.

7.18 Política de Segregación de Redes

La plataforma tecnológica de XPD que soporta los sistemas de información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El departamento de Operaciones y Desarrollo, en conjunto con el Responsable de Seguridad de la Información, es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

XPD establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la empresa.

El Responsable de Seguridad de la Información debe garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

7.19 Política de Respaldos

XPD asegura que la información contenida en bases de datos, sistemas operativos y aplicativos son resguardas de manera periódica, de acuerdo al siguiente esquema:

Tipo	Periodicidad
Bases de datos	Diario (incremental) Semanal (completo)
Sistema Operativo (configuraciones)	6 meses
Aplicativos	6 meses

La organización cuenta con un Plan de Restauración de Copias de Seguridad que es probado con el fin de asegurar que las copias son confiables, en caso de emergencia, y retenidas por un período determinado. Dicho plan se realiza en XPD de acuerdo a la siguiente tabla:

.

Tipo	Periodicidad
Bases de datos	3 meses
Sistema Operativo (configuraciones)	6 meses
Aplicativos	6 meses

Adicionalmente, XPD dispone de los recursos para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos, con el fin de acceder a la información resguardada.

El sitio alterno donde se resguardan dichas copias debe tener los controles de seguridad física.

7.20 Política de Respaldos Locales

La información de XPD debe estar respaldada en ambientes locales tales como en el Repositorio Oficial (Alfresco), así como también en los equipos de cómputo, esto es para asegurar que la información pueda ser rescatable en caso de alguna anomalía en los servidores de la organización, dichos respaldo locales se realizaran con una periodicidad mensual
Es responsabilidad del personal de XPD la organización y control de versiones de la información que se esté respaldando.

7.21 Política de Criptografía

La organización asegura que la información clasificada como reservada, confidencial o secreta es tratada de manera específica en el proceso de transportación y almacenamiento, con base en mecanismos que permitan asegurar la confidencialidad, integridad y disponibilidad de dicha información, por lo tanto:

a) Las llaves de cifrado nunca deben ser comunicadas o compartidas con ningún tercero.

b) El tamaño de la clave de cifrado (llave) para los procesos de cifrado de información contenida en medios electrónicos, debe ser evaluada y acordada por el Comité de Seguridad de la Información.

c) Los Propietarios de la información son los responsables del resguardo de las llaves de cifrado de la información.

7.22 Política de Protección contra Software Malicioso

XPD establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, que brindan protección contra código malicioso y prevención del ingreso del mismo a la red organizacional, en donde se cuenta con los controles para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Es responsabilidad del departamento de Operaciones y Desarrollo autorizar el uso de las herramientas y asegurar que éstas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, XPD define los siguientes lineamientos:

a) No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas por XPD.

- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

7.23 Política de Control de Cambios

Para minimizar los riesgos de alteración de los sistemas de información de XPD, la organización cuenta con controles durante la implementación de cambios que se reflejan en el Procedimiento de Control de Cambios de la organización.

El Procedimiento de Control de Cambios incluye las siguientes consideraciones:

a) Verificar que los cambios sean propuestos por usuarios autorizados.

b) Mantener un registro de los niveles de autorización acordados.

c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.

Por lo tanto, previo al desarrollo y mantenimiento de sistemas de XPD es necesario tomar en consideración los siguientes aspectos, a fin de cumplir con esta política:

a) Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).

b) Revisar los controles de integridad para garantizar que los activos que requieran modificaciones no son comprometidos por los cambios.

c) Obtener aprobación formal por parte del departamento de Operaciones y Desarrollo para las tareas detalladas, antes de comenzar.

d) Solicitar la revisión del Responsable de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.

e) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.

f) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.

g) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

h) Mantener un control de versiones para todas las actualizaciones de software.

i) Garantizar que la implementación se lleva a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

j) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operación.

k) Garantizar que sea el implementador quien efectúe la migración de los objetos modificados al ambiente productivo.

l) Una vez implementado el cambio, vigilar la operación del mismo a fin de identificar posibles incidentes tanto operativos como de seguridad, para atenderlos bajo los procedimientos correspondientes.

7.24 Política de Cifrado de Información de los Contribuyentes

El método de cifrado utilizado al momento de almacenar los certificados y las llaves en la base de datos del Sistema de Facturación XPD es el algoritmo AES (Advanced Encryption Standard)

Este algoritmo usa una llave binaria de 32 bytes que es representada por 64 caracteres hexadecimales obtenidos de forma aleatoria.

La llave de 32 bytes utilizada para el cifrado solo se genera una vez, ya que al tratarse de un algoritmo de encriptación simétrico, si esta llave cambia, debe modificarse en las aplicaciones que la utilicen para el cifrado y descifrado de la información.

El resultado final, cuando se aplica el algoritmo AES a un CFDI, es un dato binario, por lo que a este dato se le aplica una codificación Base64 para que este pueda ser almacenado en base de datos.

El proceso de descifrado se lleva a cabo después de que se ha autentificado mediante el usuario y contraseña del Portal.

Dicha llave solo es accesible por el personal del departamento de Operaciones y Desarrollo de XPD, que tiene acceso a los servidores de producción.

7.25 Política de Seguridad Física y Ambiental

XPD vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controla las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

La Gerencia de Operaciones XPD en conjunto con el departamento de Operaciones y Desarrollo proporcionan los recursos para ayudar a proteger y regular el estado de los controles físicos implantados en las instalaciones de XPD.

Los ingresos y egresos de personal a las instalaciones de XPD deben ser registrados; por consiguiente, el personal y terceras partes deben cumplir completamente con los controles físicos implantados.

El Responsable de Seguridad de la Información debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de las oficinas de XPD.

El personal debe portar su credencial institucional en un lugar visible mientras se encuentren en las instalaciones; en caso de pérdida de la credencial deben reportarlo a la mayor brevedad posible al Responsable de Seguridad de la Información.

En el caso del personal provisto por terceras partes, deben utilizar credencial de visitantes para su identificación y no deben intentar ingresar a áreas a las cuales no tengan autorización.

7.26 Política de Seguridad en las Operaciones

El departamento de Operaciones y Desarrollo encargados de la operación y administración de los recursos tecnológicos que apoyan los procesos de XPD, asigna funciones específicas a sus empleados, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades.

Así mismo, mantiene los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegura que los cambios efectuados sobre los recursos tecnológicos, son adecuadamente controlados y debidamente autorizados.

La Gerencia de Operaciones XPD en conjunto con el departamento de Operaciones y Desarrollo de XPD provee la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la organización, efectuando proyecciones de crecimiento y provisiones en la plataforma.

7.27 Política de Seguridad en las Comunicaciones

Para garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información, la Gerencia de Sistema, en conjunto con el Asesor de Tecnología Informática, debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de XPD, además debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

El Jefe de Desarrollo y el Jefe de Operaciones, en conjunto con el Asesor de Tecnología Informática, debe mantener las redes de datos segmentadas y debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

El departamento de Operaciones y Desarrollo, en conjunto con el Asesor de Tecnología Informática, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por XPD en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos. Además debe contar con protección entre las redes internas de la organización y cualquier red externa que esté fuera de la capacidad de control y administración de la organización.

Bajo cualquier circunstancia, el departamento de Operaciones y Desarrollo, en conjunto con el Asesor de Tecnología Informática, debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de XPD.

7.28 Política para la Adquisición, Desarrollo y Mantenimiento de Sistemas

7.28.1 Política para el Establecimiento de Requisitos de Seguridad

XPD asegura que el software adquirido y desarrollado tanto al interior del sus oficinas como por terceras partes, cumple con los requisitos de seguridad y calidad establecidos. Las áreas propietarias de sistemas de información y el departamento de Operaciones y Desarrollo incluyen requisitos de seguridad y calidad en la definición de requerimientos y, posteriormente se aseguran que éstos se encuentran generados durante las pruebas realizadas sobre los desarrollos del software construido.

a) Normas para el establecimiento de requisitos de seguridad

Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de las instalaciones.

El departamento de Operaciones y Desarrollo debe establecer metodologías para el desarrollo de software que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo, con el fin de proporcionar a los desarrolladores una visión de lo que se espera.

Las áreas propietarias de los sistemas de información, en acompañamiento con el departamento de Operaciones y Desarrollo, deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

Las áreas propietarias de los sistemas de información deben definir qué información puede ser eliminada de sus sistemas, previa autorización de la Gerencia de Operaciones XPD, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

b) Normas dirigidas a Desarrolladores Internos y Externos

Los Desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que

se desarrolle, de acuerdo con los requerimientos de seguridad y los controles deseados.

Los Desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

7.28.2 Política de Desarrollo Seguro, Realización de Pruebas y Soporte de los Sistemas

XPD vela porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad y funcionales, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.

Además, se asegura que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por XPD.

a) Normas de Desarrollo Seguro, Realización de Pruebas y Soporte de los Sistemas dirigidas a Propietarios de los sistemas de información

Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos funcionales, antes del paso a producción de los sistemas, documentado las pruebas realizadas y aprobando la liberación a producción.

Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o cambios para nuevas funcionalidades.

b) Normas dirigidas al departamento de Operaciones y Desarrollo

El departamento de Operaciones y Desarrollo debe implantar los controles para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas.

El departamento de Operaciones y Desarrollo debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.

El departamento de Operaciones y Desarrollo debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

El departamento de Operaciones y Desarrollo debe adoptar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

El departamento de Operaciones y Desarrollo debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

c) Normas dirigidas a Desarrolladores Internos y Externos

Los Desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro, por ejemplo, OWASP, SQAD, SCRUM, etc., durante el ciclo de vida de los mismos, abarcando desde el diseño hasta la puesta en marcha.

Los Desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software de XPD, dicho soporte debe contemplar tiempos de respuesta.

Los Desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

Los Desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

Los Desarrolladores deben implementar mensajes de error genéricos así como garantizar que no se divulgue información en respuestas de error que puedan vulnerar la seguridad de la organización.

Los Desarrolladores deben remover cualquier indicio que se refiera a los sistemas operativos y versiones del software utilizado.

Los Desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes.

Los Desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como éstas no sean requeridas.

Los Desarrolladores deben implementar los controles para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

Los Desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

Los Desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

7.29 Política de Relaciones con los Proveedores

El área Jurídica incluye en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios, cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de estas políticas, de todas las normas, procedimientos y prácticas relacionadas.

El Responsable del área Jurídica es responsable de notificar a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información en XPD.

Todos los proveedores de XPD que tengan una relación directa con los activos de información deben firmar un “Acuerdo de Confidencialidad de Información”, tal como se establece en la Política de Acuerdos de Confidencialidad que se presenta en este documento.

7.30 Política para la Gestión de los Aspectos de Seguridad de la Información en la Continuidad de Negocio

La Gerencia de Operaciones XPD, en conjunto con el departamento de Operaciones y Desarrollo, cuenta con un proceso de Gestión de Continuidad de Negocio para garantizar la capacidad necesaria para soportar su operación.

Para asegurar la continuidad de operación se tienen presente los procesos de la organización, considerando que el proceso de Gestión de Riesgos debe comenzar con una valoración de riesgos identificando:

a) Aquellos recursos humanos, datos, elementos de infraestructura y otros recursos, incluyendo aquellos suministrados por terceros que soportan los procesos de la organización.

b) Una lista de las vulnerabilidades potenciales, los peligros o amenazas a la organización.

c) La probabilidad estimada de que ocurran estas amenazas.

El Plan de Continuidad de Negocio (BCP, por sus siglas en inglés) definido por XPD toma en consideración las operaciones que son necesarias para la supervivencia de la organización. Además el BCP incluye:

a) El Plan de Recuperación de Desastres (DRP, por sus siglas en inglés) que se usa para recuperar una instalación que se tornó inoperable, incluyendo la reubicación de las operaciones en un nuevo lugar.

b) El Plan de Restauración que se usa para regresar las operaciones a la normalidad, ya sea en una instalación recuperada o en una nueva.

7.31 Política de Acceso a Internet

El Internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de XPD, por lo cual el uso de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxies, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Twitter, Yahoo, Youtube, correo electrónico personal y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de XPD.

b) El intercambio no autorizado de información de propiedad de XPD, de sus clientes y/o de sus empleados, con terceros.

c) La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

d) La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Jefe de Desarrollo, el Jefe de Operaciones y/o Gerente de Operaciones XPD.

e) El Asesor de Tecnología Informática debe realizar un monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los empleados y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación.

f) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

g) Los empleados y terceros, al igual que los contratistas o subcontratistas de estos, no pueden asumir en nombre de XPD, posiciones personales en encuestas de opinión, foros u otros medios similares.

7.32 Política de Correo Electrónico

Los empleados y terceros autorizados a quienes XPD les asigne una cuenta de correo deben seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del XPD.

b) Los mensajes y la información contenida en los buzones de correo son propiedad del XPD.

c) El tamaño de los buzones de correo es determinado por el Asesor de Tecnología Informática y/o Gerencia de Operaciones XPD de acuerdo con las necesidades de cada usuario.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deben ser definidos e implementados por el Asesor de Tecnología Informática.

e) No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la empresa, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Utilizar la dirección de correo electrónico de XPD como punto de contacto en comunidades interactivas de contacto social (tales como Facebook, Twitter, entre otras) o cualquier otro sitio que no tenga que ver con las actividades laborales.

- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos debe ser autorizado por el departamento de Operaciones y Desarrollo y/o Gerencia de Operaciones XPD.

b) El envío de información organizacional debe ser realizado exclusivamente desde la cuenta de correo que XPD proporciona.

c) El envío masivo de mensajes publicitarios corporativos debe contar con la aprobación de la Gerencia de Operaciones XPD y/o Gerencia de Administración. Además, para terceros se debe incluir un mensaje que le indique al destinatario cómo ser eliminado de la lista de distribución.

d) Toda información de XPD generada con los diferentes programas computacionales, que requiera ser enviada fuera de la empresa, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

e) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por XPD (identificación personal, firma con datos del empleado) y deben conservar en todos los casos el mensaje legal corporativo de privacidad.

7.33 Política de Recursos Tecnológicos

El uso adecuado de los recursos tecnológicos asignados por XPD a sus empleados y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de XPD es responsabilidad del Asesor de Tecnología Informática, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por XPD a través de la Gerencia de Operaciones XPD.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros.

c) El Asesor de Tecnología Informática debe definir y actualizar semestralmente, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d) Únicamente los empleados y terceros autorizados por el Jefe de Desarrollo, Jefe de Operaciones y/o Gerente de Operaciones XPD pueden conectarse a la red inalámbrica de XPD.

e) Solo personal autorizado por el Jefe de Desarrollo, Jefe de Operaciones XPD, puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de XPD; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por los Jefes de Operación y Desarrollo.

7.34 Política de Segregación de Funciones

Toda tarea en la cual los empleados tengan acceso a la infraestructura tecnológica y a los sistemas de información de XPD, debe contar con una definición de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de evitar el uso no autorizado o modificación sobre los activos de información de la organización.

Por tal motivo:

- Todos los sistemas deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

- Deben estar segregadas las funciones del área de Atención a Clientes y Desarrollo.

- Todas las actividades relacionadas con la segregación de funciones para el uso y manejo de los activos de tecnologías de información son responsabilidad del Asesor de Tecnología Informática y la Gerente de Operaciones XPD.

7.35 Política de Gestión de Medios Removibles

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de XPD, está autorizado para aquellos empleados cuyo perfil del cargo y funciones lo requiera, por la Gerencia de Operaciones XPD.

Los Jefes de Desarrollo y Operaciones son responsables de implementar los controles necesarios para asegurar que en los sistemas de información de XPD solo los empleados autorizados puedan hacer uso de los medios de almacenamiento removibles.

Así mismo, el empleado se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de XPD que éste contiene.

7.36 Política de Identificación de Requerimientos de Seguridad

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en XPD, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad del Asesor de Tecnología Informática.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre XPD y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información.

Es responsabilidad del Asesor de Tecnología Informática garantizar la definición y cumplimiento de los requerimientos de seguridad de la información, y en conjunto con la Gerencia de Operaciones XPD establecer estos aspectos con las obligaciones contractuales específicas.

7.37 Política para Uso de Dispositivos Personales

Los empleados de XPD pueden hacer uso de dispositivos personales para realizar actividades de trabajo, siempre que previamente haya sido autorizado por el Gerente de Operaciones XPD. Cualquier equipo móvil que contenga información de la organización debe cumplir con las siguientes medidas de seguridad:

Laptops o tabletas electrónicas:

- Activar el bloqueo del equipo y el acceso mediante contraseña.
- Contar con un antivirus actualizado.
- No instalar software que permita la explotación de riesgos que comprometan la seguridad de la información o el incumplimiento de leyes o regulaciones.
- Realizar respaldo de la información en los dispositivos de la organización cada 3 meses.
- Cumplir con la Política de Equipo Desatendido.
- No dejar el equipo en lugares que puedan ser susceptibles a robo (en lugares visibles dentro del auto, en lugares públicos, cafeterías, eventos, conferencias).
- Bloquear el equipo cuando no permanezca cerca del mismo.
- Evitar la conexión mediante WiFi en lugares públicos y de aquellas conexiones sin control de acceso.
- Informar de inmediato a la Gerencia de Operaciones XPD la pérdida o hurto del dispositivo, para que sean retirados los accesos a los servicios de red y sistemas.
- Permitir la verificación del cumplimiento de estas políticas.

Equipo Móvil:

- Acceder al equipo mediante un número, una secuencia de movimientos (Bloqueo de equipo).
- Activar el acceso mediante Número de Identificación Personal (PIN, por sus siglas en inglés) el cual se solicita cuando se reinicia el equipo o se cambia el chip.
- Únicamente se permite el uso de correo electrónico de la organización, el acceso a la red interna o sistemas de la organización está prohibido por este medio, salvo autorización expresa del Gerente de Operaciones XPD.
- Mantener el software del dispositivo actualizado, estas actualizaciones deben descargarse de un sitio de confianza.
- No utilizar el celular como medio de almacenamiento de información de la empresa.
- Notificar el robo pérdida del equipo a la Gerencia de Operaciones XPD.
- Permitir la verificación del cumplimiento de estas políticas.

7.38 Política para el Cumplimiento

La presente la Política de la Organización en Seguridad de la Información y su Políticas Específicas de Seguridad de la Información entran en vigor una vez autorizadas por el Comité de Seguridad de la Información, oficializada por la Gerencia General de XPD y cuando haya sido difundida y publicada en el repositorio oficial de la organización por el Responsable de Seguridad de la Información.

Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se debe apegar a lo estipulado en la Política para Seguridad de Recursos Humanos a fin de asegurar que se conocen las políticas de seguridad de la organización.

Las presentes políticas están alineadas con las directrices de las leyes y regulaciones existentes para el giro de negocio de la organización.

Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al Comité de Seguridad de la Información.

7.38.1 Auditorías

Con el fin de comprobar la aplicación de este documento, XPD realiza auditorías de acuerdo con el Plan de Auditoría elaborado por el Responsable de Seguridad de la Información y autorizado por el Comité de Seguridad de la Información.

Todos los hallazgos de las auditorías realizadas son comunicados a la organización, mientras que las actividades para la mitigación de los mismos son coordinadas por el Responsable de Seguridad de la Información, en conjunto con las áreas involucradas, para asegurar que todas las brechas se cierren y se alineen al cumplimiento esperado.

La organización se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes de la organización en materia de seguridad de información.
XPD se reserva el derecho de tomar medidas administrativas -de acuerdo a las Medidas Disciplinarias por Incumplimiento de la Política- en contra del personal que no dé cumplimiento a lo dispuesto en las políticas descritas en este documento.

7.39 Manejo de Desviaciones y Excepciones a las Políticas

Las solicitudes de excepciones a las políticas deben estar documentadas y justificadas teniendo la aprobación del Comité de Seguridad de la Información para considerarse válidas.

El Comité de Seguridad de la Información puede determinar el tiempo en el que las excepciones deben ser re-evaluadas y por lo tanto re-aprobadas si se considera conveniente.

7.40 Atención a Desviaciones

Los sistemas deben de ser monitoreados para detectar desviaciones respecto a la política y registrar eventos para suministrar evidencia en caso de producirse incidentes relativos a la seguridad.

7.41 Atención a Exclusiones

Las exclusiones deben estar justificadas, argumentadas y autorizadas por Comité de Seguridad de la Información.

8 Responsabilidades de Seguridad de la Información

La Política de la Organización en la Seguridad de la Información y las Políticas Específicas de Seguridad de la Información son de aplicación obligatoria a todo el personal de la empresa y/o terceros cualquiera que sea su situación contractual.

8.1 El Responsable de la Seguridad de la Información

Es el principal responsable en la definición de los criterios de seguridad de la información en XPD, por lo que debe analizar cada 6 meses o cuando exista un cambio en la infraestructura de la organización, el nivel de riesgo existente, proponiendo soluciones. Una vez autorizada la implementación de las medidas, debe coordinar con quienes corresponda su materialización.

Hace la revisión, modificación y difusión de la presente política a todos los colaboradores, además de capacitar, proponer y dar seguimiento a todos los procedimientos de seguridad para impulsar la implementación y cumplimiento de estas políticas.

8.2 El Dueño del Activo

Es la unidad organizacional o un representante que ha sido reconocido por la ley como tal.

8.3 El Custodio de la Información

Debe analizar los criterios de la clasificación y delegar la responsabilidad de manera formal al colaborador responsable con el fin de resguardar y proteger un activo de información o un conjunto de ellos.

También es quien asigna quien o quienes deben tener acceso a los activos de información.

8.4 Los Responsables de los Activos de Información

Son quienes administran, clasifican y asumen la responsabilidad de actualizar la información que maneja en el área, además autorizan la divulgación y cambios en los respectivos controles.

8.5 La Dirección

Su responsabilidad es la aprobación y autorización de las modificaciones al presente documento, reflejando su compromiso, apoyo e interés en el desarrollo de una cultura de seguridad de la información en la empresa, la revisión de la política se realiza con base a diferentes cambios en el ambiente de la empresa, debido a las circunstancias del servicio, a las condiciones legales y al ambiente técnico.

8.6 El Jefe de Desarrollo y Operaciones

Su responsabilidad es cumplir con las funciones relativas a la seguridad de los sistemas de información durante la operación, administración, comunicación y utilización de los recursos de tecnología en la empresa.

Por otra parte, tiene la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

8.7 Las Jefaturas

Su responsabilidad es asegurar que se dé la gestión de activos es sus áreas de trabajo, a fin de preservar la confidencialidad, integridad y disponibilidad de la información.

8.8 El Área de Recursos Humanos

Tiene como responsabilidad notificar al personal en su vinculación contractual con la empresa el cumplimiento de las obligaciones ligadas a estas políticas por medio del convenio de confidencialidad.

8.9 El Comité de Seguridad de la Información

Cuerpo integrado por el Gerente General de Operaciones, Gerente de Operaciones XPD, Gerencia Administrativa, Jefe de Atención a Clientes, Jefe de Desarrollo, Jefe de Operaciones, Asesor de Tecnología Informática y el Responsable de Seguridad de la Información.

El Comité de Seguridad de la Información es responsable de acordar y aprobar metodologías y procesos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la organización.

Las reuniones se llevan a cabo el último viernes de cada mes y es imperativa la asistencia de 3 de los 4 votantes presentes para que se lleve a cabo la decisión frente a los incidentes de Seguridad.

8.10 El Personal de XPD

Tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada sobre incidentes que atenten contra la seguridad de la información.

9 Medidas Disciplinarias por Incumplimiento a las Políticas

La Política de la Organización en la Seguridad de la Información y las Políticas Específicas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre el personal interno, externo y proveedores de XPD.

Por tal razón las violaciones de éstas, que sean generadas por alguno de ellos, tienen como sanción la aplicación de las medidas correctivas que están definidas en el Reglamento Interno de Trabajo de XPD.

10 Términos y Definiciones

Activo de información: Datos o información propiedad de XPD que se almacena en cualquier tipo de medio y que es considerada por la empresa como información para el cumplimiento de las actividades relacionadas sus procesos y servicios.

Clasificación del activo: Etiquetado del activo conforme a la Política de Clasificación de la Información.

Clasificación de la información: Categorización que se proporciona a la información de negocio en función de la integridad, confidencialidad y disponibilidad de la misma.

Cifrado de información de los contribuyentes: Proceso por el que una información legible se transforma mediante un algoritmo en información ilegible a fin de evitar riesgos de ser leída por terceras partes que no correspondan al contribuyente que ha contratado los servicios de XPD.

Código del activo: Clave o número de serie que identifica a los activos de propiedad de la organización.

Confidencialidad: Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

Continuidad de negocio: Actividades puestas en marcha para garantizar que las operaciones de la organización pueden continuar durante y después de un evento que afecte su operación habitual.

Control de accesos a los activos tangibles y no tangibles: Todos los activos de XPD, tangibles o intangibles, son dotados con credenciales de acceso a fin de evitar amenazas y vulnerabilidades sobre información de la organización y considerando la normatividad y regulaciones vigentes para el giro comercial al cual pertenece la compañía.

Custodio del activo: (En servidores) Es quien se encarga de supervisar la correcta administración del activo y no necesariamente hace uso del mismo. (En recursos informáticos – equipos locales) Responsable de la asignación, modificación, eliminación y manejo de los activos.

Descripción del activo: Especificaciones técnicas de los componentes del activo (procesador, memoria RAM, disco duro, sistema operativo, laptop/ desktop/ servidor/ dispositivo móvil).

Disponibilidad: Servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de la información asociados en el lugar momento y forma en que es requerido.

Dueño del activo: (En servidores) Representante legal o área de la empresa a la que pertenece el activo. (En recursos informáticos – equipos locales) Empresa, área de la empresa a la que pertenece el activo.

Equipo desatendido: El equipo de cómputo asignado a cada empleado contiene información de XPD, responsabilidad de quien la consulta o manipula por lo que cada vez que el empleado se aleje de su estación de trabajo debe aplicar el bloqueo a su equipo sin esperar que se realice de forma automática.

Eliminación de derechos de acceso: La clasificación de la información utilizada en XPD obliga a la compañía a asegurarse que los derechos de accesos a ésta sean retirada cuando algún empleado cause baja a fin de asegurar el resguardo y seguridad de la información, o bien cuando tenga cambios de puesto dentro de la organización. Esto último asegurando el acceso a lo que realmente necesario y de utilidad para el empleado.

Información: Toda forma de conocimiento objetivo con representación física o lógica explícita

IP (en servidores): Dirección de red asignada para uso de protocolos de internet para la transmisión de datos.

Integridad: Propiedad de la información que busca mantener la exactitud de la información según fue generada, sin que ésta sea modificada de manera no autorizada.

Incidente: Interrupción no planeada de un servicio o la reducción de la calidad o falla de un servicios de tecnologías de información o de un elemento de configuración que no ha impactado aún el servicio.

Incidente de Seguridad: Es el evento o serie de eventos de seguridad de la información no deseada o inesperada que tienen una significativa probabilidad de comprometer las operaciones del negocio y amenazan la seguridad de la información.

Política: Documento que describe los requisitos o reglas específicas que deben cumplirse en una organización.

Política de la Organización en la Seguridad de la Información: Cumplir con las normas y procedimientos de seguridad vigentes, mantener el resguardo y adecuada protección de la información, así como proteger los activos de las partes interesadas.

Privilegio: Es el derecho de un usuario para realizar una tarea específica, que afecta a un sistema.

Problema: Origen de uno o más incidentes del que se desconoce la causa.

Propietario o Responsable del activo: (En servidores) Es la persona que monitorea y administra el activo tomando decisiones en torno a la creación, el acceso, la modificación y la eliminación de los activos corporativos. (En recursos Informáticos – equipos locales) Persona que tiene asignado un activo y hace uso del mismo.

MAC Address (en equipos locales): Valor numérico que identifica de forma única ese dispositivo de red desde cualquier otro dispositivo del planeta.

Marca: Identificación comercial del activo.

Modelo: Versión del activo que contempla la forma, el diseño y rendimiento del activo.

Nivel de protección del activo: Evaluación de criticidad de conforme a Matriz de Gestión del Riesgo.

Riesgo: Vulnerabilidades identificadas y asociadas a una probabilidad de ocurrencia y al impacto negativos ocasionados sobre las operaciones de negocio.

Seguridad de la información: Preservación, protección y resguardo de los activos de información contra una amplia gama de amenazas para asegurar su confidencialidad, disponibilidad e integridad, de manera tal que se asegure la continuidad de las operaciones y minimizar el daño sobre los clientes, en primera instancia, y en la organización.

Serie: Código alfanumérico único asignado para identificación del activo.

Sistema de información: Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la **r**ecopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales.

Tangible: Se utiliza para nombrar lo que puede ser tocado o probado de alguna forma. En un sentido más amplio, también hace referencia a aquello que puede percibirse con precisión.

No tangible: Son aquellos que no tienen entidad física y que solo pueden ser percibidos a través del mutuo reconocimiento de ciertos derechos y obligaciones como válidas.

Tecnología de la información: Conjunto de hardware y software operados por la entidad o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la empresa para llevar a cabo sus funciones.

Tipo de activo: Clasificación del activo según su tipo hardware o software.

Ubicación Física/ Lógica: Lugar en el que permanece el activo.

Uso de contraseña: Proceso de verificación de la identidad del usuario, asegurando que éste es realmente quien dice ser, lo que le permite acceder a herramientas informáticas.

Uso de escritorio limpio: Toda la información de XPD está clasificada de acuerdo a las propiedades de la información y según se específica en la Política de Clasificación de Información, por lo que en todo momento debe de mantenerse en un lugar seguro por lo que debe mantenerse la estación de trabajo ordenada y no deben dejarse a la vista activos de información que puedan tener uso malintencionado y causar pérdidas significativas a la operación.

Uso aceptable de activos: Todos los activos de información propiedad de XPD (hardware, software, documentos, etc.) deben utilizarse de acuerdo con su razón de ser y apegado a la Política de Uso de Aceptable de los Activos.

Versión: Nombre, código o número único que indica el nivel de desarrollo y/o actualización del activo.

11 Documentos de referencia

- Norma internacional ISO/IEC 27001.
- Norma internacional ISO/IEC 20000.
- Norma internacional ISO/IEC 9001.
- Lista de obligaciones legales, normativas y contractuales.

- ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- Norma internacional ISO 22301.
- Ley Federal de Datos Personales en Posesión de Particulares.
- Matriz de controles de seguridad emitidos por el SAT.

12 Anexos

12.1 Anexo 1 Listado de aplicaciones sobre las cuales se aplican las políticas, concernientes al software, enunciadas a en este documento.

#	Sistema	Descripción	Responsable
1	Consulta CFDI's Pendientes	Consulta CFDI's pendientes por enviar al SAT.	Atención a Clientes
2	Consulta Cliente	Consulta la información de todos los clientes y su distribuidor.	Desarrollo
3	Consulta de Usuarios para el Portal de Facturación	Consulta el usuario admin del Portal de Facturación	Desarrollo
4	Update RFC	Actualiza tenant_Id en tablas de portal de facturación	Desarrollo
5	Panel de Timbrado	Consulta de subcuentas, asignación y descuento de timbres, reseteo de contraseña e historial de timbrado y movimientos de ventas.	Desarrollo
6	Servicio de Consulta de Password (distribuidores)	Para consultar contraseña de los distribuidores	Administración
7	Sistema de Consulta y Asignación de Folios	Sistema de consulta y asignación de folios	Desarrollo

#	Sistema	Descripción	Responsable
8	Sistema de Contabilidad Electrónica	Sistema para la contabilidad electrónica de CFDI's	Desarrollo
9	Sistema de Reporte de Recompras (Portal de Facturación)	Reporte de recompras para mesa de control	Administración
10	Sistema de Reporte de Recompras (XPDSystem)	Reporte de recompras para mesa de control	Administración
11	Sistema de Reporte Semanal de Nómina Excel y Recibo de Nómina Manual	Reporte total de nóminas Excel y recibo de nómina semanal del Portal de Facturación	Administración
12	Sistema de Reseteo de Contraseña de Contabilidad Electrónica	Actualiza el password de contabilidad electrónica	Desarrollo
13	Sistema de Tickets	Registro de tickets para el registro de llamadas e incidencias de soporte técnico	Desarrollo
14	Sistemas de Asignación de Addendas	Asigna addendas en el Portal de Facturación	Desarrollo
15	Portal de Facturación	Portal de Facturación	Desarrollo
16	Sistemas de Asignación de Addendas	Asigna addendas en el Portal de Facturación	Desarrollo
17	Portal de Facturación	Portal de Facturación	Desarrollo

#	Sistema	Descripción	Responsable
18	Sistema XPD System	Sistema de administración para distribuidores y mesa de control XPD	Desarrollo
19	Sistema Recibe tu Factura (validación)	Validación de XML ante el SAT	Desarrollo
20	Data Power	Sistema de administración para distribuidores y mesa de control XPD	Desarrollo