LIBERDADE DIGITAL

POLÍTICA DE SEGURIDAD

Entidad de Certificación

IDENTITY DEL PERÚ S.A.

Versión 1.0 de 29 de enero de 2025

Firmado Digitalmente por:
ROBERTO AUGUSTO CASTAÑEDA CHAVEZ DNI:42811955 RUC:20607123463
Motivo: Como representante legal
Cargo: GERENTE GENERAL
Empresa: IDENTITY DEL PERU SOCIEDAD ANONIMA
IP: 193.176.127.55
Fecha: 23/06/2025 - Hora: 20:01

Resumen

1 - INTRODUCCIÓN

Este documento él tiene poner objetivo establecer hacia pautas de seguridad qué ellos son adoptado para el EC SOLUTI LATAM PERÚ. Estas directrices proporcionan la base para las normas y procedimientos de seguridad implementados. A el cumplimiento de objetivo citado ellos son establecido tú objetivos referenciado en el siguiente punto.

2 - OBJETIVOS

EL Política de Seguridad desde EC IDENTITY DEL PERÚ S.A él tiene tú siguiente objetivos específicos :

a) colocar el alcance de seguridad desde EC IDENTITY DEL PERÚ S.A;

b) orientar, a través de sus lineamientos, todas las acciones de seguridad, para reducir los riesgos y garantizar la integridad, secreto y disponibilidad de información procedente de sistemas y recursos de información;

c) permitir el adopción de soluciones seguridad integrado; y

d) atender de referencia a auditoría, investigación y evaluación de responsabilidades.

3 - ALCANCE

EL Política de Seguridad cubre tú siguientes aspectos:

a) Requisitos de Seguridad Humano;

b) Requisitos de Seguridad Físico;

c) Requisitos de Seguridad Lógica; y

d) Requisitos de Seguridad del Características Criptográfico.

4 - TERMINOLOGÍA

Se interpretan las normas y directrices de seguridad. para que todas tus determinaciones son obligatorios y debe cumplirse íntegramente.

5 - CONCEPTOS Y DEFINICIONES

aplicar tú conceptos abajo nodo qué si se refiere el Política de Seguridad desde EC SOLUTI LATAM PERÚ :

a) Activo de Información – y el herencia compuesto poner todo tú datos y información generado y manipulado durante la ejecución de los sistemas y procesos de EC SOLUTI LATAM PERU;

b) Activo de Procesamiento – es el activo constituido por todos los elementos de hardware y software necesarios para la ejecución de los sistemas y procesos de EC SOLUTI LATAM PERU, tanto los producidos internamente como los adquiridos;

c) Control de Acceso – ellos son restricciones hacia acceso hacia información de uno sistema ejercido para el gestión de EC SOLUTI LATAM PERÚ Seguridad de la Información;

d) Custodia – Consiste en la responsabilidad de guardar un bien para terceros. Sin embargo, la custodia no permite acceder automáticamente al activo, ni el derecho de otorgar acceso a otros;

e) Bien de Acceso – y el privilegio asociado el uno cargar, persona o proceso a tener acceso el un activo;

f) Herramientas – es un conjunto de equipos, programas, procedimientos, estándares y otros recursos a través de los cuales se aplica la Política de Seguridad. de información de EC SOLUTI LATAM PERÚ;

g) Incidente de Seguridad – es cualquier evento o suceso que promueve una o más acciones que comprometa o sea una amenaza a la integridad, autenticidad o disponibilidad de cualquier activo de

EC SOLUTI LATAM PERU ;

h) Política de Seguridad – es un conjunto de lineamientos diseñados para definir la adecuada protección de los activos elaborados por los Sistemas de Información de EC SOLUTI LATAM PERU;

i) Protección de Activos – es el proceso mediante el cual se deben clasificar los activos según su grado de sensibilidad. El medio de registro de un activo de información debe recibir la misma clasificación de protección que se le otorga al activo que lo contiene;

j) Responsabilidad – se define como las obligaciones y deberes de quien ocupa un determinado rol en relación con la recopilación de información;

k) Contraseña Débil u Obvia – es aquella que utiliza caracteres fáciles de asociar con el dueño de la contraseña, o que es muy simple o pequeña, como por ejemplo: cumpleaños, bodas, nacimientos, el propio nombre, el nombre de los familiares, números secuencias de palabras simples y unidades léxicas que aparecen en diccionarios de cualquier idioma, entre otros.

6 - NORMAS GENERAL

6.1- Gestión de Seguridad

6.1.1 - La Política de Seguridad de IDENTITY DEL PERÚ S.A se aplica a todos sus recursos humanos, administrativos y tecnológicos. EL alcance del recursos citado se refiere ambos Aquellos conectado el ella como en Carácter permanente y temporal.

6.1.2 - Esta política es comunicada a todo el personal involucrado y ampliamente difundida por EC SOLUTI LATAM PERU, asegurando que todos la conozcan y la practiquen dentro de la organización.

6.1.3 - Todo el personal recibe la información necesaria para cumplir adecuadamente con lo determinado en esta política de seguridad.

6.1.4 - Se implementa un programa de concientización en seguridad de la información para asegurar que todo el personal esté informado sobre los potenciales riesgos de seguridad y exposición a los que están sujetos los sistemas y operaciones de EC SOLUTI LATAM PERU. Especialmente, el personal involucrado o que interactúa con los usuarios está capacitado sobre los ataques típicos de ingeniería social y cómo protegerse de ellos.

6.1.5 - Se documentan e implementan procedimientos para garantizar que cuando el personal contratado o los proveedores de servicios sean transferidos, reasignados, ascendidos o despedidos, todos los privilegios de acceso a los sistemas, la información y los recursos se revisen, modifiquen o revoquen adecuadamente.

6.1.6 - Previsión de un mecanismo centralizado y un repositorio para activar y mantener senderos, registros y otras notificaciones de incidentes. Este mecanismo se incluye dentro de las medidas adoptadas por un grupo encargado de responder a este tipo de ataques, para promover una defensa activa y correctiva ante los mismos.

6.1.7 - Los procesos de adquisición de bienes y servicios, especialmente Tecnologías de la Información – TI, están acordes con esta Política de Seguridad.

6.1.8 - En materia de seguridad de la información, se considera prohibido todo aquello que no esté previamente autorizado por el responsable del área de seguridad de EC SOLUTI LATAM PERU.

6.2- Gestión de Riesgos

El proceso de gestión de riesgos es revisado anualmente por EC SOLUTI LATAM PERÚ, para prevenir

riesgos, incluidos los derivados de nuevas tecnologías, con miras a desarrollar planes de acción adecuados para proteger los componentes amenazados.

6.3 Inventario de activos Todos los activos de EC SOLUTI LATAM PERU se encuentran inventariados, clasificados, actualizados permanentemente y cuentan con un administrador responsable designado formalmente.

6.4 Departamento de Continuidad de Negocio

6.4.1 Hay uno PCN implementado. EL cual y probado, para el menos uno tiempo poner año, a garantizar el continuidad de los servicios críticos.

6.4.3 El certificado EC SOLUTI LATAM PERÚ será revocado inmediatamente si un evento provoca la pérdida o compromiso de su clave privada, o de su medio de almacenamiento. En esta situación, seguirá los procedimientos detallados en su DPC.

6.4.4 Todos los incidentes serán reportados oportunamente al departamento de Cumplimiento de EC SOLUTI LATAM PERU, desde el momento en que se verifique la ocurrencia. Estas incidencias serán comunicadas de forma confidencial a las personas especialmente designadas para ello.

7 - REQUISITOS DE SEGURIDAD DE TIPO

Definición Conjunto de medidas y procedimientos de seguridad, a ser observado por los proveedores de servicios y todos los empleados, necesarios para proteger el patrimonio de EC SOLUTI LATAM PERU.

7.1 Objetivos

7.1.1 Reducir los riesgos de error humano, hurto, hurto, apropiación indebida, fraude o uso inapropiado de los activos de EC SOLUTI LATAM PERU.

7.1.2 Prevenir y neutralizar hacia comportamiento en hacia gente qué poder comprometerse el seguridad desde EC SOLUTI LATAM PERÚ .

7.1.3 Orientar y capacitar a todo el personal involucrado en la realización de trabajos directamente relacionados con EC SOLUTI LATAM PERU, así como al personal que realiza funciones de apoyo, como mantenimiento de instalaciones físicas. y la adopción de medidas de protección compatibles con la naturaleza de la función que desempeñan.

7.1.4 Orientar el proceso de evaluación de todo el personal que labora en EC SOLUTI LATAM PERU, incluso tratándose de funciones realizadas por prestadores de servicios.

7.2 Pautas

7.2.1 EL Proceso de Admisión

7.2.1.1 Se adoptan criterios estrictos para el proceso de selección de candidatos, con el fin de seleccionar, para el desde EC SOLUTI LATAM PERÚ, gente cierto es que adecuado y sin fondo qué poder comprometerse la seguridad o credibilidad desde EC SOLUTI LATAM PERÚ.

7.2.1.2 EL EC SOLUTI LATAM PERÚ No admitirá pasantes nodo ejercicio de actividades directamente relacionado con los procesos de emisión, expedición, distribución, revocación y gestión de certificados.

7.2.1.3 El empleado, empleada o servidor público firmará un término de compromiso asumiendo el deber de guardar confidencialidad, incluso cuando esté apagado, sobre todos los activos de información y procesos de EC SOLUTI LATAM PERU.

7.2.2 Deberes de rol

Hacia asignaciones de cada empleado ellos son claramente relacionado, de acuerdo con el característica de actividades desarrolladas con el fin de determinar el perfil necesario del empleado, considerando los siguientes ítems:

a) EL descripción resumen de tareas inherente a función;

b) Hacia necesidades de acceso el información sensible;

c)EL grado sensibilidad de la sector dónde el función y ejercido;

d) Hacia necesidades de contacto de servicio interno y/o externo;

e) Hacia características de responsabilidad, decisión y iniciativa inherente el función;

f) EL calificación técnica necesario hacia actuación desde función.

7.2.3 - EL Encuesta de Datos personales

Y elaborar buscar de historia desde vida público de candidato, con el objetivo de encuesta de su perfil, verificación de antecedentes y verificación del nivel educativo.

7.2.4 - EL Entrevista Admisión

7.2.4.1 Es realizada por un profesional calificado, con el fin de confirmar y/o identificar datos no detectados o no confirmados durante la investigación para el ingreso.

7.2.4.2 En la entrevista inicial se valoran las características de interés y motivación del candidato, y la información transmitida en la entrevista del candidato será únicamente de carácter público.

7.2.5 - EL Actuación de función

7.2.5.1 Los empleados tendrán desempeño evaluado y monitoreado periódicamente con el fin de detectar la necesidad de actualizaciones técnicas y de seguridad.

7.2.5.2 EL EC SOLUTI LATAM PERÚ desde el su empleados acceso hacia información, a través de el suministrar de instrucciones y orientaciones sobre medidas y procedimientos de seguridad.

7.2.6 - EL Credencial de Seguridad

7.2.6.1 Los empleados son identificados mediante una credencial, que les permite tener acceso a información sensible, de acuerdo a la clasificación del grado de confidencialidad de la información y, en consecuencia, con el grado de confidencialidad compatible con el cargo y/o función a desempeñar. realizarse.

7.2.6.2 La Credencial de Seguridad sólo es otorgada por una autoridad competente, o delegada por ésta, y se fundamenta en la necesidad del conocimiento técnico de los aspectos inherentes al ejercicio funcional y en el análisis de la sensibilidad del cargo y/o función.

7.2.6.3 El plazo máximo de validez para la concesión de una habilitación de seguridad a una persona física será de un año. Este plazo podrá ampliarse por el mismo período cuantas veces sea necesario, por acto de la autoridad concedente, siempre que la necesidad del servicio lo requiera.

7.2.7 Capacitación en Seguridad de la Información Existe un proceso mediante el cual se presenta a los empleados y proveedores de servicios la Política de Seguridad de la Información, sus reglas y procedimientos relacionados con el manejo de información y/o datos confidenciales, con el propósito de desarrollar y mantener una conciencia efectiva en materia de seguridad, así como

así como instruir su fiel cumplimiento.

7.2.8 Hacer un seguimiento nodo Actuación desde Función

7.2.8.1 Se lleva a cabo el proceso de evaluación. rendimiento de la función que documenta la observación Comportamiento personal y funcional de los empleados, realizado por su superior inmediato.

7.2.8.2 Es motivo para registrar actos, actitudes y comportamientos positivos y negativos relevantes, verificados durante la ejercicio profesional del empleado.

7.2.8.3 Los comportamientos incompatibles, o que puedan comprometer la seguridad, son investigados y comunicados a la dirección inmediata.

7.2.8.4 Los gerentes inmediatos se aseguran de que todos los empleados tengan conocimiento y comprensión de los estándares y procedimientos de seguridad establecidos.

7.2.9 EL Proceso de Cerrar

7.2.9.1 EL acceso de ex empleados hacia instalaciones, cuando necesario, será restringido hacia áreas de acceso público .

7.2.9.2 Se revocará su credencial, identificación, gafete, uso de equipos, mecanismos y accesos físicos y lógicos .

7.2.10 Proceso de Liberación El empleado firmará, antes del despido, una declaración de que no tiene ningún tipo de asunto pendiente con las distintas unidades que conforman EC SOLUTI LATAM PERU, verificando con la unidad de Recursos Humanos, y cuantas más unidades sean necesarias, la veracidad de la información.

7.2.11 - EL Entrevista de Cerrar

Se realiza una entrevista de salida para orientar al empleado sobre sus responsabilidades en el mantenimiento de la confidencialidad. de datos y/o conocimiento confidencial de sistemas críticos hacia cual el tenia acceso durante su estancia en EC SOLUTI LATAM PERÚ.

7.3 Deberes y responsabilidades

7.3.1 Deberes de empleados

7.3.1.1 Ellos son deberes del empleados:

a)Preservar el integridad y ahorrar secreto de información de qué hacer usar, bien como vigilar y proteger tú respectivos recursos de procesamiento de información;

b)para cumplir este Política de Seguridad, bajo lástima de incurrir en en el sanciones disciplinario y Frío aplicable;

c)Usar tú Sistemas de Información desde EC SOLUTI LATAM PERÚ y tú recursos el ella relacionado solo a tú fines previstos por la Gerencia de Seguridad;

d)para cumplir hacia normas específico de protección establecida hacia activos de información;

e)para mantener el personaje confidencial desde contraseña de acceso hacia recursos y sistemas desde EC SOLUTI LATAM PERÚ ;

f) no compartir, bajo cualquier forma, información confidencial con otras personas que no sean tener la autorización de acceso adecuada;

g)Responder, por cualquier y todo acceso, a los recursos de EC SOLUTI LATAM PERU así como por los efectos de dichos accesos realizados a través de de su código de identificación, o otro atributo a eso fin usado;

h)Respetar la prohibición de utilizar, inspeccionar, copiar o almacenar programas informáticos o cualquier otro material, en violación de la legislación de propiedad intelectual pertinente;

i) Comunicar hacia su superior inmediato el conocimiento de cualquier irregularidad o Desvío.

7.3.2 Responsabilidad de Gerentes

7.3.2.1 EL responsabilidad de gerentes entender, entre otros, el siguiente actividades:

a)Administrar el cumplimiento de este política de seguridad, poner parte de su empleados;

b)Identificar tú desviaciones experto y adoptar hacia medidas correctivo adecuado;

c)Impedir que los empleados despedidos o renunciados accedan a los activos de información, utilizando los mecanismos de terminación previstos en el respectivo proceso de terminación del empleado;

d)Proteger, por nivel fisico y por supuesto, el activos información y procesamiento EC SOLUTI LATAM PERÚ relacionado con su área de actividad;

e)para garantizar qué el tipo bajo su supervisión entender y llevar a cabo el obligación de proteger el Información de EC SOLUTI LATAM PERÚ;

f) Comunicarse formalmente al unidad que lleva a cabo la concesión de privilegios a usuarios de TI, qué empleados y proveedores de servicios, bajo su supervisión, que podrán acceder a información de EC SOLUTI LATAM PERU;

g)Comunicar formalmente a la unidad que otorga privilegios a los usuarios de TI, qué empleados y proveedores de servicios han sido despedidos o transferidos, para su exclusión del registro de usuarios;

h)Comunicar formalmente el unidad qué realiza el concesión de privilegios el usuarios de TÚ, Aquellos qué estén respondiendo a procesos, investigaciones o que tengan licencia, para inhabilitar a los usuarios para registrarse.

7.3.3 Responsabilidades General

7.3.3.1 Ellos son responsabilidades general:

a)Cada área que posee activos de procesamiento e información es responsable de los mismos, brindando su protección de acuerdo con la política de clasificación de información de EC SOLUTI LATAM PERU;

b)Todo tú activos de información él tiene claramente definido tú responsable para el su usar;

c)Todo tú activos de tratamiento desde EC SOLUTI LATAM PERÚ ellos son relacionado en el PCN.

7.3.4 Responsabilidades desde Gestión de Seguridad

7.3.4.1 Ellos son responsabilidades desde gestión de seguridad:

a)para establecer hacia normas de protección del activos desde EC SOLUTI LATAM PERÚ ;

b)Decidir como hacia medidas el ser enchufes nodo caso de violación de normas establecido;

c)Revisar para el menos anualmente, las reglas protector establecido;

d)Restringir y control el acceso y tú privilegios de usuarios remoto y externo;

e)Elaborar y mantener actualizado el PCN desde EC SOLUTI LATAM PERÚ ;

f) para ejecutar hacia normas de protección establecido poner este PD;

g)Detectar, identificar, registrar y comunicar violaciones o intentos de acceso no autorizados al departamento de Cumplimiento y a la Alta Gerencia de EC SOLUTI LATAM PERU;

h)Definir y aplicar, para cada usuario TI, restricciones de acceso a la Red, tales como horarios autorizados, días autorizados, entre otros;

i) Mantener registros (logs) de actividad de los usuarios de TI por un período de tiempo superior a 7 (siete) años. Los registros contendrán la hora y fecha de las actividades, identificación del usuario de TI, comandos (y sus argumentos) ejecutados, identificación de la estación local o estación remota que inició la conexión, número de procesos y condiciones de error observadas (intentos rechazados). errores de coherencia, etc.);

j) Límite el término de validez de cuentas de proveedores de servicio a período desde contratación;

k)Eliminar cuentas inactivas ;

l) Proporcionar contraseñas de cuentas privilegiadas sólo a los empleados que efectivamente necesiten los privilegios, manteniendo el debido registro y control.

7.3.5 Responsabilidades de proveedores de servicios

El contrato contiene cláusulas que cubren la responsabilidad de los proveedores de servicios en el cumplimiento de esta Política de Seguridad de la Información, sus reglas y procedimientos.

7.4 Sanciones

será aplicado hacia sanciones planificado para el legislación vigentes, según el grado de afectación y los perjuicios que se puedan encontrar, la aplicación de las sanciones podrá ser acumulativa, es decir, si se reinciden las irregularidades, se sumará la responsabilidad del causante.

8 REQUISITOS DE SEGURIDAD HACER AMBIENTE FÍSICO

8.1 Definición

El ambiente físico es el formado por todos los activos permanentes utilizados en el proceso de certificación EC SOLUTI LATAM PERÚ .

8.2 Pautas generales

8.2.1 Las responsabilidades sobre la seguridad física de los sistemas de EC SOLUTI LATAM PERU están definidas y asignadas a personas claramente identificadas.

8.2.2 EL ubicación de instalaciones y el sistema de proceso de dar un título desde EC SOLUTI LATAM PERÚ No ellos son en público identificado.

8.2.3 Se instalan sistemas de seguridad de acceso físico para controlar y auditar el acceso a los sistemas de certificación.

8.2.4 Se establecen controles duplicados sobre el inventario y las tarjetas/llaves de acceso. Se mantiene una lista actualizada del personal que posee tarjetas/llaves.

8.2.5 Las claves criptográficas bajo la custodia del tutor están físicamente protegidas contra el acceso, uso o duplicación no autorizados.

8.2.6 La pérdida de las tarjetas/llaves de acceso se reporta inmediatamente al responsable de la gestión de seguridad de EC SOLUTI LATAM PERU. Tomará las medidas oportunas para impedir el acceso no autorizado.

8.2.7 Los sistemas EC SOLUTI LATAM PERU están ubicados en un área protegida o alejados de potentes fuentes de magnetismo o interferencias de radiofrecuencia.

8.2.8 Los recursos e instalaciones críticos o sensibles se mantienen en áreas seguras, protegidas por un perímetro de seguridad definido, con barreras de seguridad y control de acceso. Están

físicamente protegidos contra accesos no autorizados, daños o interferencias. La protección proporcionada es proporcional a los riesgos identificados.

8.2.9 EL Prohibido y salida, en estos áreas o regiones dedicado, ellos son automáticamente registrado con fecha y tiempo definidos y revisados diariamente por el responsable de la gestión de seguridad de la información de EC SOLUTI LATAM PERÚ y mantenidos en un lugar adecuado y confidencial.

8.2.10 El acceso a los componentes de la infraestructura, actividad fundamental para el funcionamiento de los sistemas de aire acondicionado, como paneles de control de energía, comunicaciones y cableado, está restringido al personal autorizado.

8.2.11 Sistemas de detección de intrusión ellos son usado a monitor y registro tú golpes físico hacia Sistemas de certificación de horas de uso.

8.2.12 El inventario de todo el conjunto de activos de procesamiento se registra y se mantiene actualizado al menos mensualmente.

8.2.13 Cualquier equipo de grabación, fotografía, vídeo, sonido u otros similares sólo se utiliza con autorización y supervisión formal.

8.2.14 En las instalaciones de EC SOLUTI LATAM PERU todas las personas utilizan alguna forma de identificación visible (por ejemplo: insignia), y debe informar a seguridad de la presencia de cualquier persona no identificada o de cualquier extraño no acompañado.

8.2.15 Los visitantes a áreas seguras son supervisados. Se registran sus horas de llegada, salida y destino. Estas personas sólo acceden a áreas específicas, para fines autorizados, y dichos accesos siguen instrucciones basadas en los requisitos de seguridad del área visitada.

8.2.16 Los ambientes donde ocurren los procesos críticos de EC SOLUTI LATAM PERU son monitoreados, en tiempo real, con Imágenes grabadas a través de sistemas CCTV.

8.2.17 Existe un sistema de detección de intrusos instalado y probado periódicamente para cubrir entornos, puertas y ventanas accesibles, en entornos donde se producen procesos críticos. Las zonas desocupadas cuentan con un sistema de alarma que permanece siempre activado.

9 - REQUISITOS DE SEGURIDAD HACER AMBIENTE LÓGICO

9.1- Definición

Ambiente lógico está compuesto de todo activos de tecnología desde información EC SOLUTI LATAM PERÚ .

9.2- Pautas general

9.2.1 La información se protege según su valor, sensibilidad y criticidad. Para ello existe un estándar de clasificación de la información.

9.2.2 Los datos, informaciones y sistemas de información de EC SOLUTI LATAM PERU y bajo su custodia se encuentran protegidos contra amenazas y comportamiento No autorizado, accidental o No, de modo el reducir riesgos y garantizar el integridad, secreto y disponibilidad de estos bienes.

9.2.3 Las violaciones de seguridad se registran y estos registros se analizan periódicamente por motivos de seguridad. de carácter correctivo, legal y de auditoría. Los registros están protegidos y almacenados. según su clasificación.

9.2.4 Los sistemas y recursos que soportan las funciones críticas para la operación de EC SOLUTI LATAM PERU, aseguran la capacidad de recuperación en los plazos y condiciones definidas ante situaciones de contingencia.

9.2.5 El inventario sistematizado de toda la estructura que sirve de base para el manejo,

almacenamiento y transmisión de los activos de procesamiento deberá registrarse y mantenerse actualizado en intervalos de tiempo definidos por EC SOLUTI LATAM PERÚ.

9.3 Directrices específicas

9.3.1- Sistemas

9.3.1.1 Se identifican las necesidades de seguridad para cada etapa del ciclo de vida de los sistemas disponibles en EC SOLUTI LATAM PERU. La documentación de los sistemas se mantiene actualizada. La copia de seguridad se prueba y se mantiene actualizada.

9.3.1.2 Los sistemas cuentan con control de acceso para asegurar su uso únicamente por usuarios o procesos autorizados. La persona responsable de autorizar o confirmar la autorización está claramente definida y registrada.

9.3.1.3 Tú archivos de registros ellos son juiciosamente definido a permitir recuperación en el situaciones de fracasos, auditar situaciones de brechas de seguridad y contabilizar el uso de recursos. Los registros se analizan periódicamente, según se define en el DPC, para identificar tendencias, fallas o uso indebido. Los troncos se protegen y almacenan según su clasificación.

9.3.1.4 Se establecen y mantienen medidas y controles de seguridad para verificar críticamente la precisión, coherencia e integridad de los datos y la configuración de los sistemas y dispositivos.

9.3.1.5 Los sistemas se evalúan en cuanto a aspectos de seguridad (pruebas de vulnerabilidad y penetración) antes de ponerlos a disposición para producción. Periódicamente se evalúan las vulnerabilidades del entorno y se adoptan recomendaciones de seguridad.

9.3.2- Máquinas servidor

9.3.2.1 Se controla y protege el acceso lógico al entorno o a los servicios disponibles en los servidores. Las autorizaciones se revisan, confirman y registran de forma continua. La persona responsable de autorizar o confirmar la autorización está claramente definida y registrada.

9.3.2.2 Los accesos lógicos se registran en logs, que se analizan periódicamente. El tiempo de retención de los archivos de registro y las medidas de protección asociadas están definidos con precisión.

9.3.2.3 Se adoptan procedimientos sistematizados para monitorear la seguridad del entorno operativo, principalmente en lo que respecta a la integridad de los archivos de configuración del Sistema Operativo y otros archivos. críticos. Tú eventos ellos son almacenado en informes de seguridad (registros) de modo qué su análisis permitir la generación de pistas de auditoría a partir de estos registros.

9.3.2.4 Hacia maquinas ellos son sincronizado a permitir el seguimiento de eventos

9.3.2.5 Protección lógica adicional (criptografía) y adoptado a evitar el acceso No autorizado a información.

9.3.2.6 La versión del Sistema Operativo, así como el resto del software básico instalado en las máquinas servidor, se mantienen actualizadas, de acuerdo con las recomendaciones de los fabricantes.

9.3.2.7 Ellos son usado solo software autorizado por propia EC SOLUTI LATAM PERU en su equipo. Se deberá realizar un control de su distribución e instalación.

9.3.2.8 EL acceso remoto a máquinas servidor se lleva a cabo adoptando la mecanismos seguridad predefinida para evitar amenazas a la integridad y confidencialidad del servicio.

9.3.2.9 Procedimientos de copia seguridad (copia de seguridad) y de recuperación están documentadas, mantenidas actualizados y probados periódicamente para garantizar la

disponibilidad de la información.

9.3.3- Redes usado para el EC SOLUTI LATAM PERÚ

9.3.3.1 El tráfico de información en el entorno de la red está protegido contra daños o pérdidas, así como contra el acceso, uso o exposición indebidos, incluido el "Efecto Tempestad".

9.3.3.2 Los componentes críticos de la red local se guardan en salas protegidas con acceso físico y lógico controlado, estando protegidos contra daños, robos, hurtos y mal tiempo.

9.3.3.3 Ellos son adoptado hacia instalaciones seguridad disponible de forma innato a nosotros activos de tratamiento de la red.

9.3.3.4 La configuración de todos los activos de procesamiento se verifica en la instalación inicial, de modo que se detecten y corrijan las vulnerabilidades inherentes a la configuración estándar que se encuentran en estos activos en su primera activación.

9.3.3.5 Servicios vulnerable recibir nivel de protección adicional .

9.3.3.6 EL usar de contraseñas y enviado el uno política específico a su gestión y uso.

9.3.3.7 El acceso lógico a los recursos de la red local se realiza a través de un sistema de control de acceso. El acceso lo otorga y mantiene la administración de la red, en función de las responsabilidades y tareas de cada usuario.

9.3.3.8 El uso de cualquier mecanismo capaz de realizar pruebas de cualquier naturaleza, como, por ejemplo, monitorear los datos, sistemas y dispositivos que componen la red, se utiliza con base en una autorización y supervisión formal.

9.3.3.9 La conexión a otros entornos de red y los cambios internos en su topología y configuración están formalmente documentado y mantenido, de forma el permitir registro histórico, teniendo el autorización desde administración de redes y gestión de seguridad. El diagrama topológico, la configuración y el inventario de recursos se mantienen actualizados.

9.3.3.10 Los informes de seguridad (registros) están definidos para ayudar en el manejo de desviaciones, recuperación de fallas, contabilidad y auditoría. Los registros se analizan periódicamente y el periodo de análisis establecido es el más breve posible.

9.3.3.11 Ellos son adoptado protecciones fisicas adicional por los recursos de red considerada crítica.

9.3.3.12 Protección lógica adicional y adoptado a evitar el acceso no autorizado a la información.

9.3.3.13 EL infraestructura de interconexión lógica y protegido contra daño mecánica y sin conexión autorizado.

9.3.3.14 EL alimento eléctrico a el red ubicación y separado desde red convencional, ser observado las recomendaciones de los fabricantes de los equipos utilizados, así como las normas ABNT aplicables.

9.3.3.15 Se monitoriza el tráfico de información con el fin de verificar su normalidad, así como detectar situaciones anómalo desde el punto de vista de la seguridad.

9.3.3.16 Se observan problemas relacionados con la propiedad intelectual al copiar software o archivos desde otras ubicaciones.

9.3.3.17 La información sensible, corporativa o que pueda causar daño a EC SOLUTI LATAM PERU está protegida y no será enviada a otras redes sin la protección adecuada.

9.3.3.18 Todo servicio de red No explícitamente autorizado será obstruido o desactivado.

9.3.3.19 Mecanismos de seguridad articulaciones en sistemas de protección de acceso (cortafuegos) ellos son usado para proteger las transacciones entre las redes externas y la red interna de EC SOLUTI LATAM PERU.

9.3.3.20 Los registros de eventos se analizan periódicamente, lo más rápido posible y a

intervalos de momento apropiado.

9.3.3.21 Se adopta un estándar de seguridad para todo tipo de equipos servidores, considerando aspectos físicos y lógicos.

9.3.3.22 Todo tú recursos considerado crítico para el entorno de red, y que cuentan con mecanismos control de acceso, utilice dicho control.

9.3.3.23 EL ubicación del servicios articulaciones en sistemas de protección de acceso (cortafuegos) y resultante de uno análisis de riesgos. Como mínimo se consideran los siguientes aspectos: requisitos de seguridad definidos por el servicio, objetivo del servicio, público objetivo, clasificación desde información, forma de acceso, frecuencia de actualizar de contenido, forma administración de servicios y volumen de tráfico.

9.3.3.24 Los entornos de red considerados críticos están aislados de otros entornos de red para garantizar un nivel adicional de seguridad.

9.3.3.25 Las conexiones entre las redes de EC SOLUTI LATAM PERU y redes externas estarán restringidas únicamente a aquellas destinadas a la realización de los procesos.

9.3.3.26 Se activan las conexiones de red: primero, sistemas con función de certificación; segundo, sistemas que ejecutan hacia funciones de archivos y repositorio. Si este No para posible, emplear controles de compensación, como el uso de proxies que se implementan para proteger los sistemas que realizan la función de certificación contra posibles ataques.

9.3.3.27 Los sistemas que realizan la función de certificación están aislados para minimizar la exposición contra intentos de comprometer la confidencialidad, integridad y disponibilidad de las funciones de certificación.

9.3.3.28 EL llave de proceso de dar un título desde EC SOLUTI LATAM PERÚ y protegido de acceso no autorizado, a garantizar su confidencialidad e integridad.

9.3.3.29 La seguridad de las comunicaciones intra e interredes, entre los sistemas de las entidades del ICP-Brasil, está garantizada por el uso de mecanismos que garantizan la confidencialidad e integridad de la información transmitida.

9.3.3.30 Se implementan herramientas de detección de intrusiones para monitorear redes críticas, alertando periódicamente a los administradores de red sobre intentos de intrusión.

9.3.4- Control de acceso lógico (basado en contraseñas)

9.3.4.1 Los usuarios y aplicaciones que necesitan acceso a los recursos de EC SOLUTI LATAM PERU son identificados y autenticados.

9.3.4.2 El sistema de control de acceso mantiene calificaciones y registros actualizados que permiten contabilizar el uso, auditar y recuperar en situaciones de falla.

9.3.4.3 Ninguno usuario es capaz de obtener tú derechos de acceso de otro usuario.

9.3.4.4 La información que especifica los derechos de acceso de cada usuario o aplicación está protegida contra modificaciones no autorizadas.

9.3.4.5 EL archivo de las contraseñas son cifrado y tener el acceso revisado.

9.3.4.6 Las autorizaciones se definen según la necesidad de realizar funciones (acceso motivado) y considerando el principio de privilegios mínimos (tener acceso únicamente a recursos o sistemas necesarios para realizar tareas).

9.3.4.7 Las contraseñas son individuales, secretas, intransferibles y están protegidas con un nivel de seguridad compatible con la información asociada.

9.3.4.8 EL sistema de control de acceso tiene mecanismos qué prevenir el generación de contraseñas

débil o obvio.

9.3.4.9 Se definen adecuadamente las siguientes características de las contraseñas: conjunto de caracteres permitidos, longitud mínima y máxima, período máximo de validez, método de intercambio y restricciones específicas.

9.3.4.10 EL distribución de contraseñas hacia usuarios de TÚ (inicial o No) y hecho de forma seguro. EL contraseña Cuando el sistema lo genera, el usuario de TI lo intercambia en el primer acceso.

9.3.4.11 El sistema de control de acceso permite al usuario cambiar su contraseña cuando lo desee. El cambio de una contraseña bloqueada sólo se realizará después de que el usuario haya sido identificado positivamente. La contraseña ingresada no se mostrará.

9.3.4.12 Se adoptan criterios para bloquear o inhabilitar a los usuarios según un período predefinido sin acceso y sucesivos intentos fallidos de acceso.

9.3.4.13 EL sistema de control de acceso solicitará nuevo autenticación después bien tiempo de inactividad desde sesión (se acabó el tiempo).

9.3.4.14 El sistema de control de acceso muestra una pantalla inicial con un mensaje indicando que el servicio sólo puede ser utilizado por un usuario autorizado. Al conectarse, el sistema muestra información sobre el último acceso al usuario.

9.3.4.15 El registro de actividades (logs) del sistema de control de acceso se define con el fin de coadyuvar en el tratamiento de temas de seguridad, permitiendo la contabilidad de uso, auditoría y recuperación en situaciones de falla. Los registros se analizan periódicamente.

9.3.4.16 Los usuarios y administradores del sistema de control de acceso son formal y expresamente conscientes de sus responsabilidades, mediante la firma de un término de compromiso.

9.3.5 Computación tipo

9.3.5.1 - Hacia estaciones de trabajar, incluido equipo portátil o pararse solo, y información ellos son protegido contra daños o pérdidas, bien como acceso, usar o exposición indebida .

9.3.5.2 Los equipos que realizan operaciones sensibles reciben protección adicional, considerando los aspectos lógico (control de acceso y cifrado) y físico (protección contra robo o sustracción de equipos o componentes).

9.3.5.3 Se adoptan medidas lógicas de seguridad relativas a la lucha contra virus, copias de seguridad, control de acceso y uso de software no autorizado.

9.3.5.4 Hacia información almacenada en medio electrónica ellos son protegido contra daño, robos o robos, Se adoptan procedimientos de respaldo, definidos en un documento específico.

9.3.5.5 La información confidencial, corporativa o cuya divulgación podría causar daño a EC SOLUTI LATAM PERU, sólo se utiliza en equipo desde EC SOLUTI LATAM PERÚ dónde Ellos eran generado o en esos poner ella autorizado, con controles adecuados .

9.3.5.6 El acceso a la información cumple con requisitos de seguridad, considerando el entorno y forma de uso de la misma. equipos (de uso personal o colectivo).

9.3.5.7 Tú usuarios de TÚ, usar justo software graduados para el fabricante a nosotros equipo desde EC SOLUTI LATAM PERU, cumpliendo con los estándares ICP-Brasil y la legislación de software.

9.3.5.8 EL EC SOLUTI LATAM PERÚ establece tú aspectos de control, distribución y instalación de software usado.

9.3.5.9 EL impresión de documentos confidencial y hecho bajo supervisión de responsable. Tú informes impreso están protegidos contra pérdida, reproducción y uso no autorizado.

9.3.5.10 EL inventario de recursos y mantenido actualizado.

9.3.5.11 Tú sistemas en usar pedido nuevo autenticación después bien tiempo de inactividad desde sesión (se acabó el tiempo).

9.3.5.12 Hacia medios de comunicación ellos son eliminado de forma seguro, cuando No son más necesario. Trámites formal Se deben definir medidas para la eliminación segura de los medios a fin de minimizar los riesgos.

9.3.6 Luchar el Virus de Computadora

Tú procedimientos de luchar el procesos destructivo (virus, caballo de troya y gusanos) ellos son sistematizado e incluyen servidores, estaciones de trabajo, equipos portátiles y microcomputadoras independientes.

10 - REQUISITOS DE SEGURIDAD DE RECURSOS CRIPTOGRÁFICO

10.1- Requisitos General a Sistema Criptográfico desde EC SOLUTI LATAM PERÚ

10.1.1 EL sistema criptográfico desde EC SOLUTI LATAM PERÚ y comprendido como ser uno sistema compuesto de:

a) documentación normativo específico de cifrado en servicio hacia directivas de AC/B Foro;

b) colocar de requisitos de cifrado;

c) proyectos y metodos de implementación;

d) módulos implementado de hardware y software;

e) ajustes relativo el algoritmos criptográfico y demasiado algoritmos miembros de uno proceso criptográfico;

f) procedimientos adoptado a gestión de llaves criptográfico;

g) metodos adoptado para probar de robustez de figuras y detección de violaciones de estos.

10.1.2 Todo el documentación, referente el definición, descripción y especificación del componentes del Los sistemas criptográficos utilizados en EC SOLUTI LATAM PERU están alineados con las mejores prácticas del mercado, con los requisitos del programa WEBTRUST FOR CERTIFICATION. PRINCIPALES AUTORIDADES Y CRITERIOS y demás lineamientos establecidos por el INDECOPI.

10.1.3 EC SOLUTI LATAM PERU es responsable de monitorear los desarrollos tecnológicos y, cuando sea necesario, actualizar los estándares y algoritmos criptográficos, con miras a mantener la seguridad de la infraestructura, siempre y cuando no exista recomendación contraria del mercado, en particular señalada por la CA. /B Foro.

10.1.4 Todo parámetro crítico, cuya exposición indebida comprometa la seguridad del sistema criptográfico EC SOLUTI LATAM PERU, será almacenado encriptado.

10.1.5 Los aspectos relevantes relacionados con la criptografía en el ámbito de EC SOLUTI LATAM PERU se detallan en documentos específicos.

10.2- Claves criptográficas

10.2.1 Los procesos que involucran las claves criptográficas de EC SOLUTI LATAM PERU se realizan por un número mínimo y básico de las personas, así como están sujetos a mecanismos de control consideró adecuado por el programa WEBTRUST y lineamientos del INDECOPI.

10.2.2 Hacia gente, el qué si se refiere el artículo anterior, ellos son formalmente designado para el liderazgo competente, según el funciones realizado y el correspondiente grado de privilegios,

como esto como él tiene su responsabilidades definido explícitamente.

10.2.3 Tú algoritmos de creación y de reemplazo de las llaves criptográfico usado nodo sistema criptográfico de EC SOLUTI LATAM PERU son los recomendados por las mejores prácticas del mercado, especialmente el Foro CA/B.

10.2.4 Los diferentes tipos de claves criptográficas y sus funciones en el sistema criptográfico de EC SOLUTI LATAM PERU se explican en el DPC o en una PC específica.

10.3- Transporte de Información

10.3.1 El proceso de transporte de claves criptográficas y demás parámetros del sistema de cifrado EC SOLUTI LATAM PERU tiene asegurada la integridad y confidencialidad, mediante el uso de soluciones criptográficas específicas.

10.3.2 Ellos son adoptado recursos VPN (redes privado virtual), basado en criptografía, para el intercambio de información sensible, a través de redes públicas, entre las redes SOLUTI utilizadas por EC SOLUTI LATAM PERU.

11 - AUDITORÍA Y VIGILANCIA

11.1 Las actividades de EC SOLUTI LATAM PERU están asociadas al concepto de confianza. Los procesos de auditoría representan instrumentos qué facilitar el percepción y transmisión de confianza el comunidad de usuarios, dado que el objetivo de estos procesos es verificar la capacidad de EC SOLUTI LATAM PERU para cumplir con los requisitos de la legislación vigente.

12 - GESTIÓN DE RIESGOS

12.1– Definición

12.1.1 Proceso que tiene como objetivo proteger los servicios y operaciones de EC SOLUTI LATAM PERU, mediante la mitigación o transferencia de riesgos, lo que sea más viable económica (y estratégicamente). Se deben identificar los siguientes puntos principales:

a) EL qué él debe ser protegido;

b) Análisis de riesgos (Contra OMS o contra qué él debe ser protegido);

c) Evaluación de riesgos (Análisis desde relación coste/beneficio).

12.2- Fases Principal

12.2.1 - EL gestión de riesgos consiste de siguiente fases principales:

a) Identificación del recursos el ser protegido – hardware, red, software, datos, información personal, documentación, suministros;

b) Identificación del riesgos (amenazas) – qué ellos pueden ser natural (p.ej. tormentas, inundaciones), causado por personas (por ejemplo, ataques, robos, vandalismo, errores o negligencias) o de cualquier otro tipo (por ejemplo, incendios);

c) Análisis del riesgos (vulnerabilidades e impactos) – identificar hacia vulnerabilidades y tú impactos asociados;

d) Evaluación de riesgos (probabilidad de ocurrencia): estudio de la probabilidad de que ocurra la amenaza, estimación el valor de probable prejuicio. Este evaluación el puede ser hecho con base en información histórico o en mesas internacionales ;

e) Tratamiento de riesgos (medidas a adoptar): cómo afrontar las amenazas. Las principales

alternativas son: eliminar el riesgo, prevenir, limitar o transferir pérdidas o aceptar el riesgo;

f) Monitoreo de eficacia del controles adoptado a minimizar tú riesgos identificado;

g) Revalorización periódico del riesgos en intervalos de tiempo No superiores a 1 (uno) año.

12.3- Riesgos relacionado

Tú riesgos evaluado a el EC SOLUTI LATAM PERÚ entender, entre otros, tú siguiente:

SEGMENTO	RIESGOS
Datos e información	Indisponibilidad, Interrupción (pérdida), interceptación, modificación, fabricación, destrucción.
Características Humanos	Omisión, error, negligencia, imprudencia, mala praxis, negligencia, corrupción pasiva, sabotaje y pérdida de conocimiento.
Red	Seco, acceso no autorizado, interceptación, ingeniería social, identidad falsificado, reenviar de mensaje, violación de integridad, indisponibilidad o negativa de servicio y indisponibilidad hardware /red/conectividad.
Hardware	Indisponibilidad, modificación de configuraciones, interceptaciones (hurto o hurto) y averías.
Software y Sistemas	Interrupción/indisponibilidad (eliminación), interceptación, modificación, fallos, errores lógicos, ausencia o brecha de seguridad, falta de documentación adecuada o suficiente.
Características criptográfico	Fallos en el Ciclo de Vida del Certificado Digital, gestión inadecuada de claves criptográficas, errores de hardware criptografía, uso inadecuado de algoritmos (errores en el desarrollo y uso) y manipulación y destrucción inadecuada del material criptográfico.

12.4- Consideraciones General

12.4.1 Se documentan los riesgos que no pueden mitigarse y se estudian soluciones y controles compensatorios alternativos, dependiendo de su probabilidad de ocurrencia y sus respectivos impactos (financieros, operativos y de degradación de la imagen de EC SOLUTI LATAM PERÚ).

12.4.1.1 Uno eficaz gestión del riesgos permite decidir si el costo de prevenir uno riesgo (medida de protección) es mayor que el costo de las consecuencias del riesgo (impacto de la pérdida).

12.4.1.2 La gestión de riesgos de EC SOLUTI LATAM PERÚ cuenta con la participación e involucramiento de sus altos directivos. gerencia y accionistas.

12.5- Implementación de Gestión de Riesgos

EL gestión de riesgos en EC SOLUTI LATAM PERÚ y conducido de acuerdo con el metodología definido nodo Programa de Seguridad SOLUTI, que cubre todos los temas relacionados y se basa en marcos de mercado acreditados como el del Comité de Organizaciones Patrocinadoras de la Comisión Treadway – COSO, ISO 31000 e ISO 27001.

13 - DEPARTAMENTO DE CONTINUIDAD HACER NEGOCIO

13.1- Definición

Plan cuyo objetivo es mantener en operación los servicios y procesos críticos de EC SOLUTI LATAM PERU, en caso de desastres, ataques, fallas y mal tiempo.

13.2- Directrices generales

13.2.1 Deben estar disponibles sistemas y dispositivos redundantes para garantizar el funcionamiento continuo de los servicios críticos de manera oportuna.

13.2.2 Se establece para EC SOLUTI LATAM PERU un Plan de Continuidad de Negocio – PCN, un Plan de Respuesta a Incidentes y un Plan de Recuperación de Desastres. Estos planes prevén, como mínimo, el tratamiento adecuado de los siguientes eventos:

a) Condiciones a activar el plan;
b) Trámites de contingencia/emergencia;
c) Procedimiento de retroceder;
d) Trámites de restauración;
e) Línea de tiempo a mantenimiento del plano;
f) Requisitos de conciencia y educación;
g) Responsabilidades individuales ;
h) Objetivo de tiempo de recuperación (RTO, o cuánto tiempo llevará establecer operaciones) y Objetivo de punto de recuperación (RPO, o cuánta pérdida de datos se permite en el PCN);
i) Pruebas regular de planes contingencia ;
j) EL planear mantener o restaurar las operaciones comerciales de AC de manera oportuno, después la interrupción o falla de procesos comerciales críticos;
k) Definición de requisitos a almacenar materiales criptográfico críticos en uno ubicación alternativa;
l) Definición de interrupciones aceptable de sistema y uno tiempo de recuperación;
m) Frecuencia a realización de copias de respaldo;
n) Distancia entre hacia instalaciones de recuperación y el sitio web principal desde ANTES DE CRISTO; y
o) Procedimientos para proteger sus instalaciones después de un desastre y antes de restaurar un ambiente seguro en el sitio original o remoto.

13.2.2.1 Nodo tratamiento constante nodo PCN él debe ser consideró:

a) Compromiso desde llave privado desde EC IDENTITY DEL PERÚ S.A. ;
b) Invasión y/o penetración de sistema y desde red interno desde EC IDENTITY DEL PERÚ S.A ;
c) Incidentes de seguridad físico y lógica;
d) Indisponibilidad desde Infraestructura;
e) Fraude que se produzca en el registro de usuarios, emisión, envío, distribución, revocación y gestión de certificados;
f) Compromiso de control de seguridad en cualquier evento referenciado nodo PCN;
g) Notificación el comunidad de usuario, si para el caso;
h) Revocación del certificados afectado, si para el caso;
i) procedimientos para interrupción o suspensión de servicios y investigación;
j) análisis y escucha de senderos de auditoría; y
k) relación con el público y con medio de comunicación, si es el caso.

13.2.3 Todo tipo directamente involucrado con todo el ciclo de gestión y ejecución del Plan de Continuidad de Negocio y Ciclo de Prueba, denominado PCN – Plan de Continuidad de Negocio, recibe formación y orientación específica, para que sea posible afrontar este tipo de incidencias de la mejor forma posible.