Arquitectura y Seguridad

Aplicaciones GreyPhillips

GreyPhillips es una plataforma en línea, cuya arquitectura está basada en una estructura de servidores dedicados y distribuidos que permiten el balanceo de cargas de los diversos dominios correspondientes a cada cliente, siendo que las bases de datos se encuentran en estos servidores, ya sean estos compartidos o especializados por cliente según el requerimiento del alcance de cada cuenta.

El desarrollo de la plataforma está basado en Microsoft .Net y usando componentes especializados de diferentes fabricantes, entre ellos Google y Telerik para realizar funciones avanzadas de mapeo y para la experiencia de usuario a través de las interfaces web, la plataforma está estructurada de manera tal, que se conserven las normativas de seguridad exigidas, además de administrar el acceso controlado para cada cuenta de cada cliente.

Según su categorización, cada cliente puede tener acceso por medio de servicios web individuales, así como utilización de la plataforma a través del sub dominio especializado, técnica que permite evaluar rendimiento independiente para cada cuenta, ayudando al análisis de desempeño y registro de la utilización a vistas de recomendaciones futuras para mantener el correcto rendimiento de la plataforma.

El acceso remoto está completamente denegado, por tal motivo, el acceso directamente a las bases de datos se encuentran todos los puertos bloqueados, con excepción del puerto 443 para propósitos de uso de regulado.

Toda la plataforma está construida para evitar ataques de denegación de servicio o de inyección de consultas SQL, siendo evaluada cada instrucción recibida y no permitiendo instrucciones concatenadas.

La plataforma puede ser utilizada por los sistemas de terceros, que interactúan con esta a través de los servicios web, mismos que requieren de parametrización a través de usuario y contraseña administrables por cada cliente desde el panel de control de la plataforma principal.

Capa de Seguridad

La capa de seguridad de acceso a funcionalidades está definida desde la estructura de permisos del sistema, siendo administrable indistintamente de la base de datos y motor que se estén utilizando, permitiendo la portabilidad y la gestión de la estructura y datos, misma razón por la que se mantiene separada la capa de la lógica del sistema de la de datos, no requiriendo funcionalidades escritas directamente sobre las bases de datos, como Jobs o procedimientos almacenados, excluyendo las tareas relacionadas al mantenimiento y respaldos, simplificando la portabilidad y la administración técnica relacionada a cada cuenta y proyecto.

Los accesos a través de los servicios web son también bitacorizados de manera que se pueda medir y controlar el uso y abuso de las funcionalidades por parte de terceros, esta estrategia permite establecer políticas para la correcta gestión y baja saturación de las plataformas.

Cuando la plataforma se utiliza dentro de la infraestructura provista se pueden tener ambientes altamente controlados respecto al acceso de los datos, siendo este un compromiso inherente a nuestros servicios, sin embargo, cuando las plataformas son solicitadas para instalaciones on-premise, es decir, instaladas en la infraestructura propietaria del cliente, estos controles pasan a estar en manos de los encargados de tal infraestructura, desligando completamente la responsabilidad de la vigilancia de la acceso y de las compuertas habilitadas como accesos remotos y accesos directos a las bases de datos, en estos escenarios la plataforma es incapaz de mantener un control sobre acciones maliciosas, sin embargo, la plataforma establece firmado electrónico para cierto tipo de transacciones, las cuales deben ser mantenidas intactas por su naturaleza, a pesar del acceso directo a la información, el sistema puede validar y bloquear acceso información alterada, como es el caso de las tareas dentro de los flujos de proceso ya que esto se consideran te alta sensibilidad y dentro del contexto de la información confidencial.

También son instalados certificados de seguridad de orden obligatorio, para darle cumplimiento a las normativas del acceso seguro a la plataforma ya sea por medio de las interfaces web o por medio de los servicios web disponibles.

Los aplicativos Windows, formularios web, aplicaciones para dispositivos, o cualquier mecanismo que requieran de acceso a las bases de datos, ya sea para agregar actualizar, eliminar o consultar información deben utilizar esos accesos controlados vía servicios web, siendo necesario siempre: el nombre del dominio, usuario y contraseña y en algunos casos es requerido el Token cuyo tiempo de vida es de no más de cinco minutos, especialmente útil para transacciones oficiales como los relacionados a facturación electrónica.

Según la clasificación de la información, cuando esta entra en el rango de información sensible puede ser eliminada automáticamente, de tal manera que se evite el acceso directo posterior una vez que haya cumplido con su función. Cuando se trabaja con información temporal, habitualmente para el envío de estados de cuenta bancarios o información transmitida a través del correo electrónico o mensajes de texto, también pueden ser establecidos parámetros de seguridad como la destrucción del contenido de la información de manera automática una vez ejecutado el proceso de envío, manteniendo únicamente la información referencial relacionada.

Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes en Lógica Digital del Oriente S.A, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

Debe ser conocida y cumplida por todo el personal sea cual fuere su nivel jerárquico, rol dentro de la organización o tercerización.

Términos y Definiciones

A los efectos de este documento se aplican las siguientes definiciones relacionadas a la Seguridad de la Información y se entiende como la preservación de las siguientes características:

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se especifican las siguientes definiciones:

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Evaluación de Riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

Política de Seguridad de la Información

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida. Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Objetivo

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales. Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se aplica en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

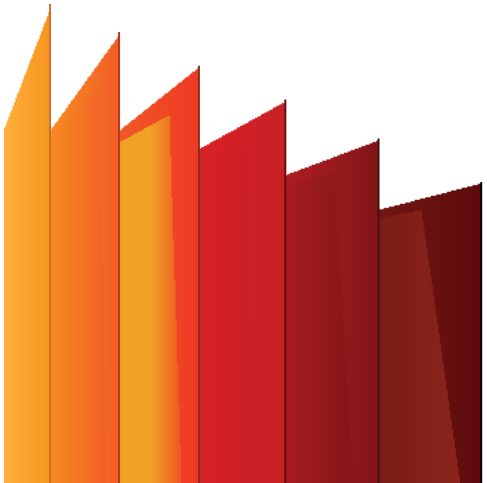
Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

Organización de la Seguridad: Orientado a administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para controlar su implementación.

Clasificación y Control de Activos: Destinado a mantener una adecuada protección de los activos del Organismo.

Seguridad Física: Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del Organismo.

Gestión de las Comunicaciones y las Operaciones: Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.



Control de Acceso/General

Orientado a controlar el acceso lógico a la información.

Desarrollo y Mantenimiento de los Sistemas Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

Administración de la Continuidad de las Actividades del Organismo Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Clasificación y Control de Activos

El Organismo debe tener conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico), mobiliario, lugares de emplazamiento, etc.

Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.). Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su sensibilidad y criticidad. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

Responsabilidad Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

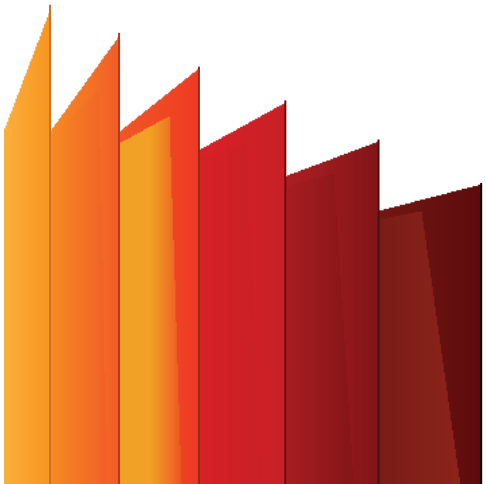
Clasificación de la información para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

Confidencialidad

0- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del Organismo o no. PUBLICO
1- Información que puede ser conocida y utilizada por todos los empleados del Organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo, el Sector Público Nacional 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 podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional 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 del Organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

Integridad

0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Organismo.
1- Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para el Organismo, el Sector Público Nacional o terceros.
2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.
3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Organismo, al Sector Público Nacional o a terceros.



Disponibilidad

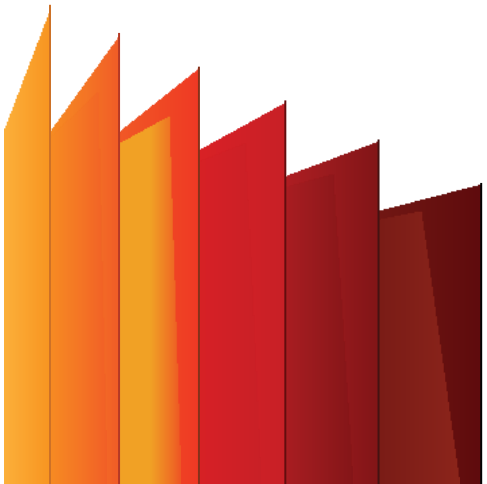
0. Información cuya inaccesibilidad no afecta la operatoria del Organismo.
1. Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.
2. Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.
3. Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.). Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

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



SEGURIDAD FISICA

Generalidades

La seguridad física brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del Organismo. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del Organismo, de accesos físicos no autorizados.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del Organismo. Dichos procesos deben ser ejecutados bajo normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al Organismo, pero situado físicamente fuera del mismo ("housing") así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Organismo ("hosting").

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

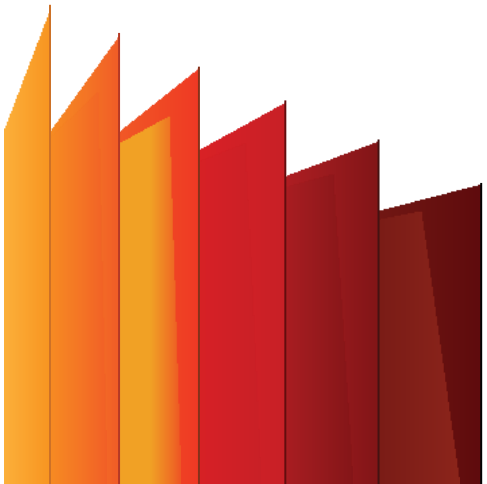
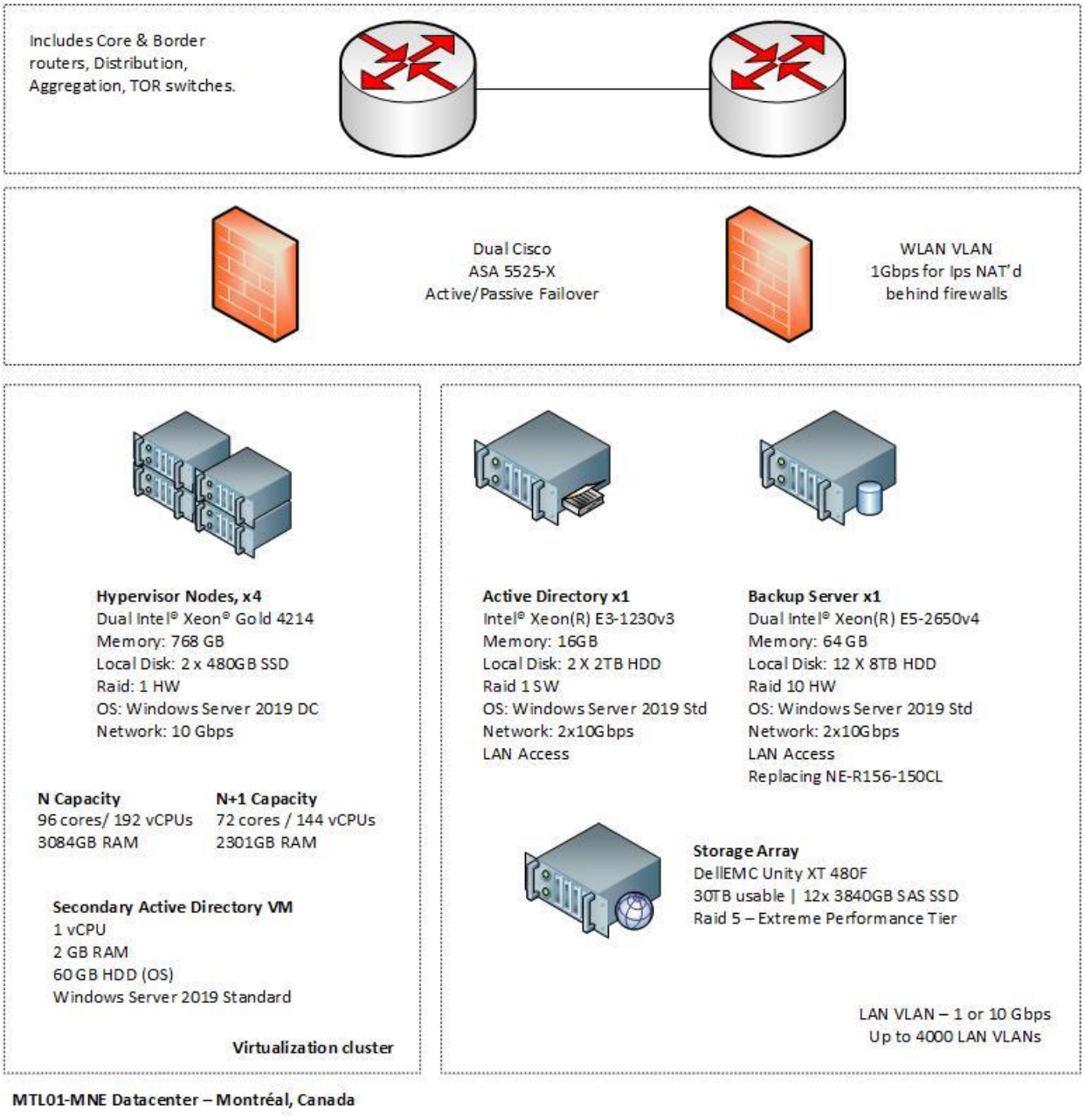


Diagrama de la arquitectura física (VPR)

La infraestructura de red es un entorno completamente compartido en el que sólo los servidores y los dispositivos están dedicados a clientes individuales. Cada rack está compuesto por una pila de switches top of rack agrupados en un modo de chasis virtual para los equipos de última generación, que actualmente se basan en Juniper.

A su vez, cada pila TOR está conectada a una pila de agregación mediante enlaces ascendentes redundantes. Los enlaces ascendentes de agregación se aprovisionan inicialmente a 10 Gbps por pila de bastidores y se aumentan en función de los tipos de servidores aprovisionados y del consumo de ancho de banda.

Por último, las pilas de agregación se conectan de forma redundante a los enrutadores de tránsito del centro de datos para el acceso ascendente suministrado por la infraestructura del centro de datos.



Políticas Área Protegidas

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

b) Establecemos que los sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

c) Las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.

d) Se agregará protección externa a las ventanas, en particular las que se Separar las instalaciones de procesamiento de información administradas por el Organismo de aquellas administradas por terceros.

e) Acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.

f) Sistemas de alarma con monitoreo 24/7 365 días del año para detección por robo o intrusión, situación de pánico, incendio o emergencia médica. Aislamiento de las Áreas solo Personal Autorizado.

Se controlarán las áreas las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados. Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso, desde el exterior del Organismo, sólo al personal autorizado.

b) Registrar el material entrante al ingresar al sitio pertinente.

Políticas de Escritorios y Pantallas Limpias

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

b) Guardar bajo llave la información sensible o crítica del Organismo cuando no está en uso, especialmente cuando no hay personal en la oficina.

c) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña).

d) Retirar inmediatamente la información sensible o confidencial, una vez impresa

SEGURIDAD LOGICA

Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre sí, tanto dentro del Organismo como con terceros fuera de él.

Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan. Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

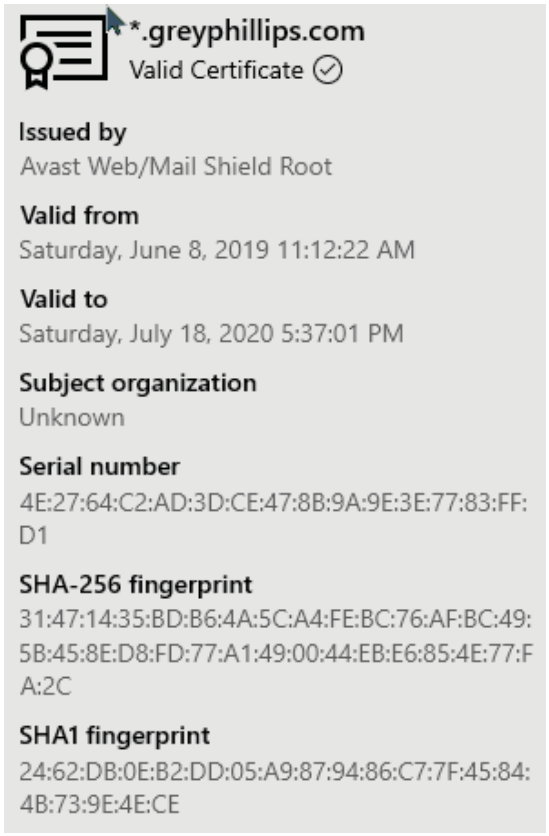
Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Alcance

Todas las instalaciones de procesamiento y transmisión de información del Organismo.

Nos respaldamos con un certificado SSL a nivel Web.

Además, poseemos un servidor dedicado administrado por Técnicos especializados en Canadá, donde administramos las comunicaciones y bases de datos de nuestros clientes.



Políticas

Separación entre Instalaciones de Desarrollo e Instalaciones de Soporte

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferiblemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo. Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

Gestión de Instalaciones Externas

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes cuestiones específicas.

Requerimientos de Seguridad en Contratos de Tercerización:

a) Identificar las aplicaciones sensibles o críticas que convenga retener en el Organismo.
b) Obtener la aprobación de los propietarios de aplicaciones específicas.
c) Identificar las implicancias para la continuidad de los planes de las actividades del Organismo.
d) Especificar las normas de seguridad y el proceso de medición del cumplimiento.
e) Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad.
f) Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Protección Contra Software Malicioso

Controles Contra Software Malicioso

El Organismo Informático definirá controles de detección y prevención para la protección contra software malicioso. El personal designado por éste, implementará dichos controles.

Se desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por el Organismo.
b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del Organismo, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

Resguardo de la Información

Se determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información. Se dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del organismo.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

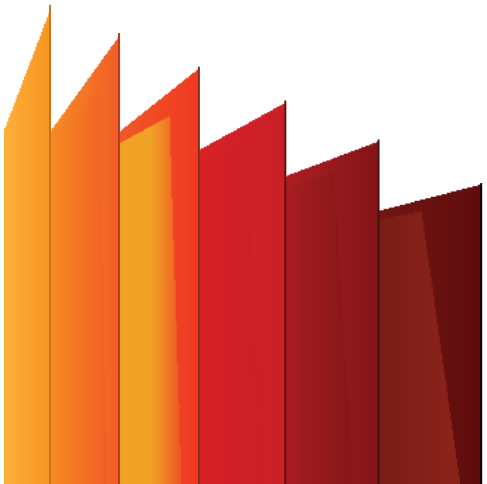
a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal.
d) Probar periódicamente los medios de resguardo.
e) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Administración de Medios Informáticos Removibles

Se implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos.

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio Reutilizable que hade ser retirado o reutilizado por el Organismo.
b) Requerir autorización para retirar cualquier medio del Organismo y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.



Eliminación de Medios de Información

El responsable del Área Informática, junto con el responsable de Seguridad Informática definirán procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

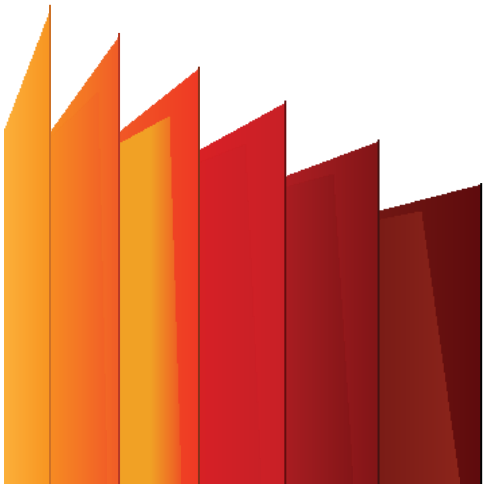
Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.
b) Voces u otras grabaciones.
c) Papel carbónico.
d) Informes de salida.
e) Cintas de impresora de un solo uso.
f) Cintas magnéticas.
g) Discos o casetes removibles.
h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
i) Listados de programas.
j) Datos de prueba.

Acuerdos de Intercambio de Información

Cuando se realicen acuerdos entre organizaciones para el intercambio de información, se especificarán el grado de sensibilidad de la información del Organismo involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
b) Procedimientos de notificación de emisión, transmisión, envío y recepción.
c) Normas técnicas para el empaquetado y la transmisión.
d) Pautas para la identificación del prestador del servicio de correo.
e) Responsabilidades y obligaciones en caso de pérdida de datos.
f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
g) Términos y condiciones de la licencia bajo la cual se suministra el software.
h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
i) Normas técnicas para la grabación y lectura de la información y del software.
j) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves, criptográficas, etc.).



Control de Accesos

Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

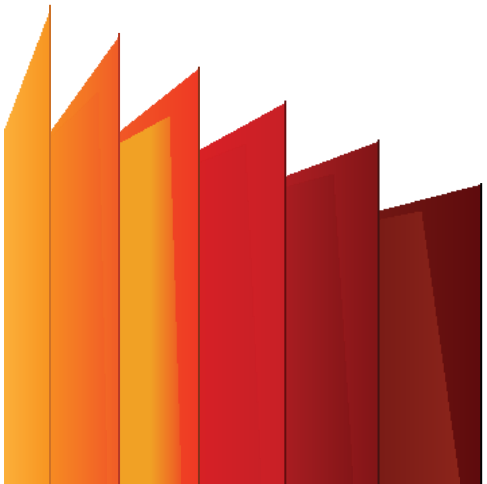
Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del Organismo, cualquiera sea la función que desempeñe.

Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.



Política de Control de Accesos

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

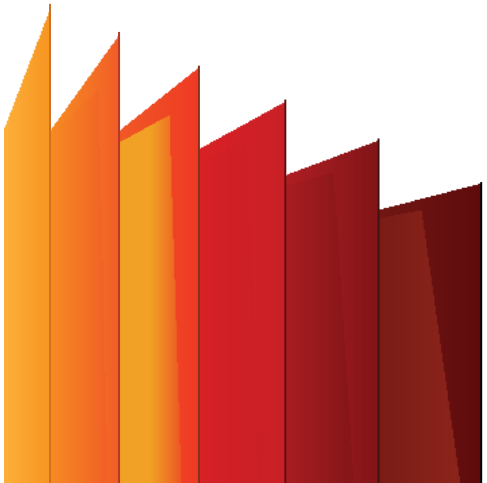
a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificar toda la información relacionada con las aplicaciones.
c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes.
d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

Registro de Usuarios/Administración de Accesos de Usuarios

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Se definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del Organismo, por ejemplo, que no compromete la separación detareas.
d) Mantener un registro formal de todas las personas registradas para utilizar el servicio (Guardado en Basede datos).
e) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.



Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Se deben tener en cuenta los siguientes pasos:

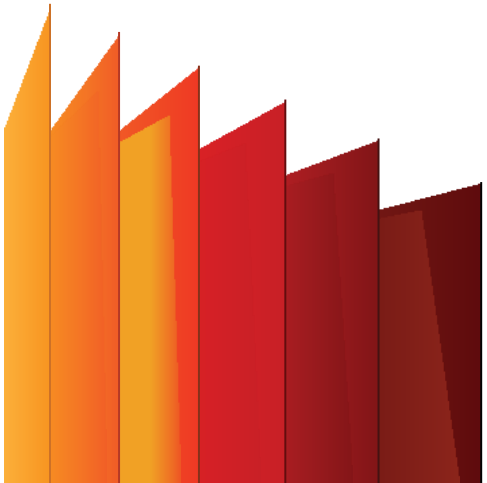
a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo, el requerimiento mínimo para su rol funcional.
c) Mantener un proceso de autorización y un registro de todos los privilegios asignados.
d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el responsable del Activo de Información de que se trate, que: (Recomendaciones)
    1. Sean fáciles de recordar.
    2. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.



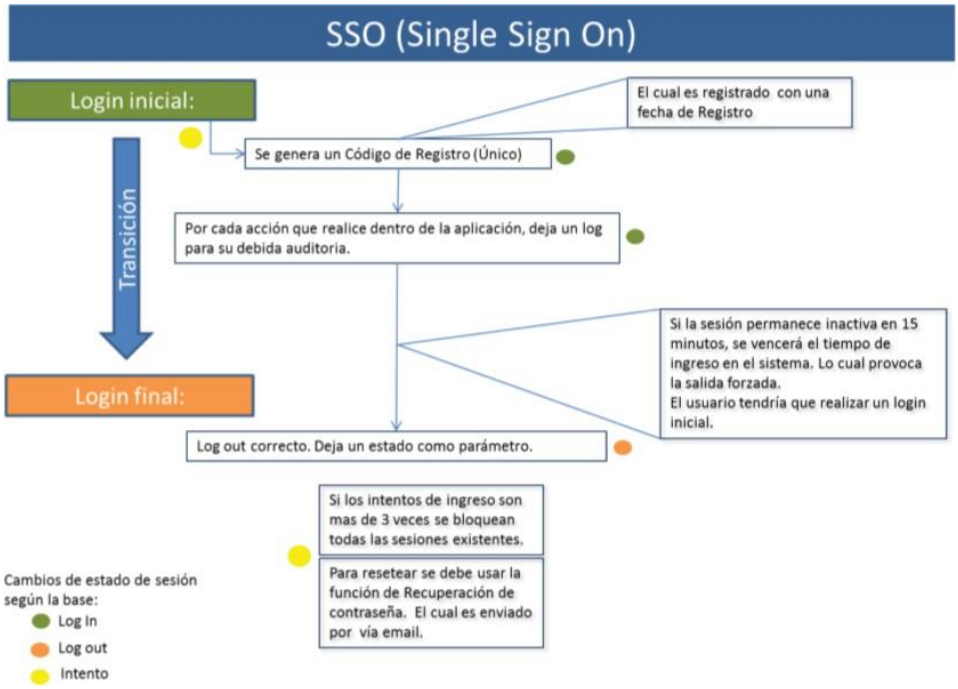
Nivel de seguridad SSO (Single-Sign-On)

La implementación de un sistema de SSO para el ingreso de usuarios a las funciones vía web también llamado Web Access Management (Web-AM), son estandarizadas según el protocolo de seguridad correspondiente.

Aplicado con los estándares que lo respaldan. El cual habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

El nivel de seguridad SSO cubre nuestras plataformas en línea: **Cloud, Portales**

de Clientes/Proveedores y comercio electrónico.



En breve una diagramación en resumen del proceso.

Con respecto a la imagen anterior, Se ingresar si:

- No existe una sesión activa con el mismo número de Código de Registro (Único)
- Si no está bloqueado.

Bloquea si:
- Hay más de 3 intentos fallidos sin importar el código de sesión

Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

- SHA-1 = 160 bits ECDSA

Política de Utilización de Controles Criptográficos

El Organismo establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

a) Se utilizarán controles criptográficos en los siguientes casos:

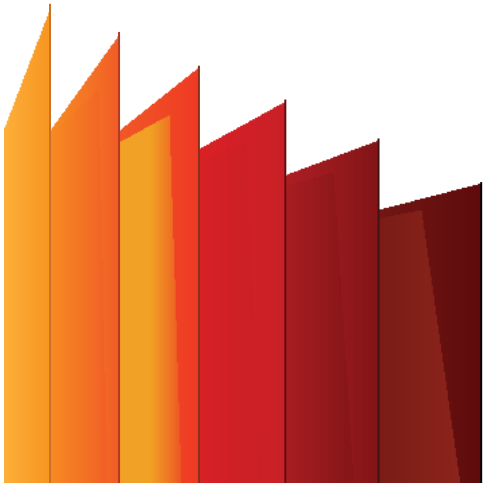
1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera del ámbito del Organismo.
3. Para el resguardo de información.

b) Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el responsable de Seguridad Informática, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la Política del Organismo en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología.



Políticas Corporativas
Junio 2023

www.greyphillips.com

Por mucho tiempo, la seguridad se ha equiparado a estar cerrado, pero cuando se trata de ecosistemas móviles esa transformación ha tenido que ir de plataformas aisladas a plataformas abiertas que fomenten la innovación y permitan la interoperabilidad dentro de un marco de seguridad y confianza. El esquema de seguridad de GreyPhillips está construido para proteger a los usuarios y a las organizaciones a mantener su información segura.

25 YEARS

GreyPhillips
Make IT happen