Políticas IT

IT
Olam Uruguay
Oct/2016
uy-it@olamnet.com

Introducción

El propósito de este documento es definir las políticas y procedimientos involucrados con el fin de mantener un nivel adecuado de seguridad de la información.

A continuación se describirán los distintos elementos que tienen participación directa en nuestro esquema de seguridad de la información detallando las políticas y procedimientos de cada uno.

Active Directory

Con el fin de mantener un control centralizado de los distintos recursos informáticos de la organización, ya sean usuarios, equipos y datos, se implementó un Dominio en Active Directory con Windows Server.

Las políticas definidas para este punto son:

- Los equipos cliente, ya sean desktop o laptop, deben de tener un sistema operativo de Microsoft Windows Professional 7 o superior.
- Los equipos servidor deben de tener un sistema operativo Windows Server 2008 o superior.
- Todo equipamiento ya sea cliente o servidor debe está dado de alta en el dominio.
- Todos los usuarios deben de tener una cuenta de usuario creada en el dominio local para acceder a cualquier recurso
- Los usuarios no deben ser administradores de sus equipos.
- El usuario debe cambiar su contraseña la primera vez que se habilita en el sistema
- El usuario debe cambiar la contraseña cada 45 días
- La cuenta se bloquea luego de 3 intentos fallidos

Complejidad de la contraseña: Debe tener al menos 8 caracteres, no puede ser parte del nombre o apellido, debe contener algún número o carácter especial, recuerda 10 anteriores

Administración de Cuentas de Usuario

La administración de las cuentas de usuario es realizada por el departamento de IT.

Mediante la creación de una cuenta de usuario para cada persona autorizada a ingresar al dominio, es posible identificar los distintos actores del sistema y definir qué acceso tendrá cada uno a los recursos informáticos de la organización, la estructura organizada en grupos para facilitar la administración de los usuarios.

Las políticas definidas para este punto son:

- Todos los usuarios de Montevideo deben de tener una cuenta de usuario creada en el dominio.
- Los usuarios de las oficinas en los campos que acceden a software y recursos compartidos deben tener un usuario en el dominio.
- Cada usuario debe tener los permisos mínimos necesarios para poder realizar sus tareas laborales.
- Las cuentas son personales y no deben de existir cuentas de usuario grupales. Esto implica que cada persona debe de tener su propia cuenta de usuario y no que varias personas utilicen una misma cuenta de usuario.
- Cuando una persona deja de tener vínculo con la organización, su cuenta de usuario debe ser des-habilitada por un periodo prudencial y luego eliminada, una vez que se confirma que no hay necesidad de activarla nuevamente.
- La política de definición del nombre de usuario es utilizar la primera letra del nombre, seguida por el apellido de la persona.

El procedimiento definido para este punto es:

- Recursos humanos notifica al departamento de IT vía correo electrónico cuando se producen cambios en la planilla de empleados de la organización, ya sea por el ingreso de personal o el alejamiento del mismo. Luego el departamento de IT define el nuevo usuario en el dominio y se pone en contacto con el usuario para darle instrucciones de cómo utilizar el mismo. En caso que sea la baja de un usuario, la misma es des-habilitada luego de recibir la notificación y luego el departamento se comunica quien corresponda con el fin de verificar que no se necesite ninguna información perteneciente a dicho usuario. Luego de un periodo prudencial, dicha cuenta es eliminada.

Correo y Lync

- Las cuentas de correo y Lync son creadas y administradas por US Support.
- Todo usuario puede tener una cuenta de correo si las tareas que tiene que cumplir así lo requieran.
- Los usuarios que lo necesiten pueden tener una cuenta de Lync
- Las cuentas de correo son personales y no deben de existir cuentas de correo grupales. Esto implica que cada persona debe de tener su propia cuenta de correo y no que varias personas utilicen una misma cuenta de correo.
- Cuando una persona deja de tener vínculo con la organización, su cuenta de correo debe ser eliminada o redirigida a quien corresponda por un periodo prudencial, y luego eliminada.

  El procedimiento definido para este punto es:

- El responsable de determinado sector solicita al departamento de IT la creación de una nueva cuenta enviando un formulario definido con los datos del usuario, IT solicita a US Support la creación de la misma reenviando los datos. Cuando se recibe la confirmación, IT notifica al solicitante y se comunica con el usuario para darle instrucciones de uso de la misma. En caso de ser una baja, se modifica la contraseña de la cuenta de correo. Luego el departamento de IT se comunica con los encargados de la persona con el fin de definir a quien deben ser redirigidos los correos recibidos por dicha cuenta de correo y además agrega una respuesta automática que notifique a los remitentes que dicha cuenta ya no está operativa indicando donde deben de enviar los correos de ahora en más. Luego de un tiempo prudencial se solicita a US Support la eliminación de la cuenta.

Administración de Acceso a Datos

En este punto se distinguen dos tipos de acceso a datos, que son los siguientes:

1. El acceso a archivos almacenados en carpetas compartidas en los servidores de la organización.
2. El acceso a información contenida en las aplicaciones que son utilizadas por la organización.

Acceso a Archivos Almacenados

A continuación se describirán las políticas y procedimientos definidos para el acceso a archivos almacenados en carpetas compartidas en los servidores. La administración de la seguridad de acceso a las carpetas compartidas es responsabilidad del departamento IT.

Las políticas definidas para este punto son:

- Cada carpeta compartida debe de tener definida los permisos de acceso para la misma, los cuales son asociados a un grupo previamente definido en el Active Directory. Siempre se definen dos grupos por carpeta compartida donde un grupo tiene acceso de modificación y otro solamente de lectura.
- Los permisos de acceso para los distintos usuarios se manejan a través de la membresía de dicho usuario al grupo correspondiente de acceso a dicha carpeta.
- Las modificaciones de pertenencia a dichos grupos las realiza el departamento de IT, el cual previamente realiza las averiguaciones y obtiene la autorización del dueño de datos correspondiente.

Los procedimientos definidos para este punto son:

- El requerimiento de alta, baja o modificación de acceso a un recurso compartido puede generarse por un usuario o dueño de datos. Dependiendo de quién genere dicho requerimiento, el departamento de IT procede a verificar el mismo con el dueño de datos y realizar la modificación correspondiente.

Acceso a Aplicaciones

Actualmente existen cuatro aplicaciones que son utilizadas por personal de la organización, a continuación se enumeran las mismas y se describe su funcionalidad:

- **GIRH:** esta aplicación es utilizada por el departamento de recursos humanos para la administración de la plantilla de trabajo de la organización y es utilizada para la liquidación de sueldos de los funcionarios y exportación de asientos para el sistema contable. Solamente acceden a ella cuatro usuarios de Montevideo.
- **Magma:** esta aplicación es un ERP, la cual es utilizada para la administración contable de las empresas Gimley, Lembay y Jorbely, es utilizada tanto por usuarios en Montevideo como administrativos en los campos, quienes acceden vía Remote Desktop con su usuario del dominio.
- **Livestock:** esta aplicación es para el reporte y administración del ganado vivo y todo lo que tiene que ver con los consumos de las unidades de Gimley y Lembay, es utilizada tanto por el personal de los campos como por los usuarios de Montevideo, es de acceso web.

Las políticas definidas para este punto son:

- Cada persona autorizada debe tener un usuario único de acceso a la aplicación.
- Cada usuario debe tener los mínimos privilegios necesarios dentro de la aplicación para cumplir con sus responsabilidades laborales.
- La administración de los usuarios de las aplicaciones queda a cargo de un responsable o dueño de aplicación, quien es la persona responsable de la administración de los usuarios de dicha aplicación. A continuación se detalla el responsable de la administración de acceso de cada aplicación:
    - GIRH: la persona encargada de la definición de los usuarios y sus perfiles es HR.
    - Magma: la persona encargada de la definición de los usuarios y sus perfiles es F&A.
    - Livestock: la persona encargada de la definición de los usuarios y sus perfiles es IT.

Los procedimientos definidos para este punto son:

- El requerimiento de alta, baja o modificación de acceso a una aplicación puede generarse por un usuario o dueño de aplicación. Dependiendo de quién genere dicho requerimiento, el responsable de dicha aplicación procede a verificar el mismo y realizar las modificaciones correspondientes.

Respaldos

Mediante una tarea programada los usuarios de la oficina central respaldan sus archivos en una unidad compartida en el servidor de archivos. Esta unidad está incluida en la política de respaldo general que va a cinta y a disco.

Los procedimientos definidos para este punto son:

- Para cada usuario se genera una carpeta en la unidad del servidor y se le aplican los permisos para que solo él pueda escribir y leer en dicha carpeta. Se le configura en su máquina un script programado para ejecutar la tarea de respaldo.

Firewall

Debido a los diversos riesgos que representa tener una conexión a Internet hoy día, es necesario tener equipamiento que permita implementar políticas de seguridad donde existan dichas conexiones, con el fin de proteger la red interna de accesos no autorizados y diversos riesgos provenientes de Internet.

Las políticas definidas para este punto son:

- En cada sitio donde exista una conexión a Internet se debe instalar un equipo de gateway para proteger a la red interna. Dichos equipos deben ser preferentemente Firewall´s o Routers que soporte el filtrado de paquetes.
- La administración de dicho equipamiento es responsabilidad del departamento de IT.
- Dicho equipamiento debe ser revisado periódicamente para verificar su funcionamiento y configuración, así como también la necesidad de aplicarle actualizaciones pertinentes.
- No se deben de configurar accesos externos más allá de los aprobados por el departamento de IT en conjunto con los encargados de los distintos sitios.
- Las políticas de seguridad implementadas en los equipamientos deben ser de denegar todo con excepción de lo permitido. Y que el tráfico permitido sea el mínimo necesario para cumplir con los requerimientos operativos.
- Luego de realizar cambios en las configuraciones de los equipamientos, se debe realizar un respaldo de la configuración del mismo.

Los procedimientos definidos para este punto son:

- Cuando surge un requerimiento, el departamento de IT evalúa su necesidad y factibilidad. Luego solicita la autorización correspondiente con el encargado del sitio para proceder con los cambios necesarios. Luego de que el cambio quede implementado el departamento de tecnología procede a realizar el respaldo de la configuración del equipo.

Antivirus

Debido a que los equipos de Gateway no son capaces de proteger contra todos los riesgos provenientes de Internet, es necesario tener instalado una protección contra virus, malware y spyware en los equipos de las redes internas que son susceptibles de dichos ataques.

Para este propósito se eligió el producto OfficeScan de TrendMicro el cual brinda protección contra lo mencionado anteriormente, además de centralizar la administración de los clientes antivirus e brindar una consola central donde se pueden ver los eventos, estado y riesgos detectados por los equipos que tengan el cliente antivirus instalado.

Las políticas definidas para este punto son:

- Todo equipo desktop, laptop y servidor que tenga instalado un sistema operativo de Microsoft, debe tener instalado el cliente antivirus.
- La administración de la infraestructura de antivirus es responsabilidad del departamento de IT.
- El departamento de IT debe realizar una revisión semanal del estado y alertas de los clientes a través del servidor de antivirus.

Los procedimientos definidos para este punto son:

- Está configurado que semanalmente se realiza un escaneo completo de todos los equipos que tienen instalado el antivirus.
- El departamento de tecnología es responsable de instalar dicho cliente en todos los equipos de la organización.
- El departamento de tecnología realiza dos revisiones semanales verificando que no hayan clientes con versiones viejas del cliente antivirus y de los resultados de los riesgos detectados por el mismo, realizando el seguimiento del mismo en los casos pertinentes.

Acceso Remoto

Existen casos en que personal de la empresa tiene la necesidad de conectarse a la red interna de la organización fuera del horario o que no estén en un sitio de la red interna. En dichos casos es posible dicha conexión mediante el protocolo PPTP a un equipo de Gateway de la red de Montevideo.

Estos tipos de conexiones se permiten, pero son manejados como excepciones y se permiten solamente con la autorización correspondiente de un encargado del sector.

Las políticas definidas para este punto son:

- Todas las conexiones remotas deben solicitar datos de autenticación para establecer la conexión con el equipo Gateway. Luego de esta autenticación el usuario además debe de autenticarse en el dominio para acceder a los recursos del mismo.
- Solamente al personal autorizado se le concede credenciales de autenticación para

conexiones remotas.

- La administración de las cuentas de acceso remoto son responsabilidad del departamento de IT.

Los procedimientos definidos para este punto son:

- El requerimiento de alta o baja de acceso remoto puede generarse por un usuario o encargado de sector. Dependiendo de quién genere dicho requerimiento, el departamento de IT procede a verificar el mismo con el encargado del sitio y realizar la modificación correspondiente.
- Siempre que el departamento de recursos humanos notifica sobre el alejamiento de un empleado se revisa que dicha persona tenga credenciales de acceso remoto y en caso afirmativo se eliminan dichas credenciales.

Seguridad Física del Centro de Cómputos

Actualmente contamos con dos centros de cómputos, uno de producción y otro de contingencia, que están ubicados en:

- Producción: Bolivia 1322 – Carrasco Montevideo
- Contingencia: Plaza Independencia 755 Piso 10 – Ciudad Vieja Montevideo

Las políticas definidas para este punto son:

- Solamente personal autorizado tiene acceso al centro de cómputos.
- Cada centro de cómputo debe tener un extintor de incendio apropiado.
- Debe contar con la refrigeración adecuada

Los procedimientos definidos para este punto son:

- Solamente el personal del departamento de IT cuenta con llave de acceso para los centros de cómputos.
- En cada ubicación, se cuenta con una copia de la llave. La cual se encuentra bajo la responsabilidad de una persona de confianza.

Redes Remotas

Tenemos 11 oficinas distribuidas en el interior del país, que tiene la necesidad de acceder a los datos, recursos y aplicaciones existentes en la red central. Dichas oficinas tienen un enlace dedicado MPLS que está conectado a modo de sub-red con Montevideo. Tomando como red central a la red de Montevideo, se denominan redes remotas a todas las sub-redes de los

distintos sitios que necesitan estar conectadas permanentemente con la red central. Al conjunto de todas las redes remotas y la red central se le denomina Intranet. Estas oficinas cuentan con una salida a Internet independiente a la sub-red con Montevideo, todo tráfico que no es parte del negocio sale por esa conexión.

Las políticas definidas para este punto son:

- Todo sitio que necesite acceder a los datos, recursos y aplicaciones de la organización debe pertenecer a la Intranet de la organización.
- Todo sitio debe contar con su propia salida a Internet
- El mantenimiento y administración de dicha intranet está a cargo del departamento de IT.
- Siempre que sea factible y viable dicha conexión debe ser del tipo punto a punto y provista por el proveedor de servicios de Internet elegido por la organización.

Los procedimientos definidos para este punto son:

- Siempre que surge el requerimiento de conexión a la intranet de una nueva sub-red remota, el departamento de tecnología analiza dicho requerimiento y las alternativas de conexión juntamente con su factibilidad. Luego de seleccionar y obtener la aprobación correspondiente en caso de que implique un incremento de los costos operativos de la organización, el departamento de tecnología procede a implementar dicha conexión.

Tolerancias a Fallas

Con el trascurso del tiempo, la organización se vuelve cada vez más dependiente de sus recursos informáticos y tecnológicos. Es debido a esto que se torna necesario la implementación de tolerancia a fallas en ciertos puntos clave de la infraestructura tecnológica de la organización.

Las políticas definidas para este punto son:

- La definición, implementación y configuración de qué equipamiento debe soportar tolerancia a fallas es responsabilidad del departamento de tecnología de la organización.
- En caso de una falla en el suministro eléctrico, cada centro de cómputos cuenta con una UPS cuya autonomía es de una hora y es capaz de soportar todo el equipamiento dentro del centro de cómputos.
- En caso de falla en un equipo de comunicaciones central de las redes de los sitios más importantes, es que se cuenta con equipamiento redundante de comunicaciones instalado en alta disponibilidad.
- En caso de una falla en los enlaces de comunicaciones entre los sitios de la Intranet, dichas oficinas cuentan con una segunda salida a Internet que les permite seguir conectados

Los procedimientos definidos para este punto son:

- El departamento de tecnología es el responsable de implementar las políticas de tolerancia a fallas definida previamente. Para esto se analiza cada infraestructura para identificar los puntos que necesitan una tolerancia a falla y luego a implementar la misma. En caso que se necesite realizar una inversión para agregar la tolerancia contra una falla, se procede a solicitar la autorización y aprobación de la misma. En caso afirmativo el departamento de tecnología implementa dicha tolerancia a falla.