



Qindel - Política de Seguridad

v 1.9

Qindel
12/12/2019

Table of Contents

| | |
|--|----|
| 1 Alcance | 3 |
| 2 Versiones | 4 |
| 3 Introducción | 5 |
| 4 Comité de Seguridad | 6 |
| 5 Activos, riesgos y vulnerabilidades | 7 |
| 5.1 Activos de nuestros clientes..... | 7 |
| 6 Acceso físico | 9 |
| 7 Acceso Lógico a la infraestructura interna de Qindel..... | 10 |
| 7.1 Acceso a las aplicaciones..... | 10 |
| 7.2 Autenticación de usuarios, autorización y Contabilidad | 10 |
| 7.2.1 Autenticación de usuario | 10 |
| 7.2.2 Autorización de usuario | 10 |
| 7.2.3 Cuentas de usuario | 11 |
| 7.2.4 Política de Contraseñas..... | 11 |
| 7.2.5 Creación, actualización y borrado de usuarios..... | 11 |
| 7.3 Aplicaciones especiales..... | 11 |
| 8 Acceso a Internet | 12 |
| 8.1 Políticas:..... | 12 |
| 9 Backup y Recuperación | 13 |
| 9.1 Política de retención | 13 |
| 9.2 Política de almacenamiento | 13 |
| 9.3 Recuperación de desastres | 13 |
| 10 Políticas de usuario y requerimientos | 14 |
| 10.1 Políticas de usuario..... | 14 |
| 10.2 Equipos de usuario | 15 |
| 11 Autor | 16 |

1 Alcance

El objetivo de este documento es definir las políticas de seguridad básicas para Qindel

2 Versiones

| <i>Ver</i> | <i>Author</i> | <i>Date</i> | <i>Change</i> |
|------------|---------------|-------------|--|
| 1.9 | Juan Zea | 12/12/2019 | Política de almacenaje en CPD |
| 1.6 | Nito Martínez | 1/8/2017 | Política para equipos obsoletos |
| 1.5 | Nito Martínez | 15/6/2017 | Política de equipos de usuario |
| 1.4 | Nito Martínez | 10/4/2017 | Enhance end user security, reference external document |
| 1.3 | Nito Martínez | 26/9/2011 | End user security |

| <i>Ver</i> | <i>Author</i> | <i>Date</i> | <i>Change</i> |
|------------|---------------|-------------|---------------------------------|
| 1.1 | Nito Martínez | | Backups y períodos de retención |
| 1.0 | Nito Martínez | | Versión Inicial |

3 Introducción

Este documento trata de configurar la política de seguridad básica en Qindel. El objetivo de esta política de seguridad es minimizar los riesgos para la organización manteniendo los procedimientos tan sencillos como sea posible.

Este documento se debe complementar con procedimientos detallados alineados con la política documentada aquí

La política de seguridad se enfoca en tres areas principales:

- Acceso físico
- Acceso a IT interno
- Acceso a IT externos (a través de internet)

Cada área debe desarrollar procedimientos estándar que dependan de la tecnología utilizada en dicha área en particular.

4 Comité de Seguridad

Este comité es responsable de aprobar las politicas de seguridad-

Cualquier excepción a esta política debería ser específicamente aprobada por el comité de seguridad o por negocio.

El comité de seguridad debe ser designado por la dirección y se puede contactar con él mediante la dirección de correo "comite-seguridad-qindel@qindel.com"

5 Activos, riesgos y vulnerabilidades

Esta es una lista de algunos activos internos que esta política trata de proteger:

- Información financiera
- Documentos internos
- Mensajes de Email y mensajería inmediata
- Código fuente del software y paquetes binarios
- Documentación interna de recursos humanos
- Hardware

Los riesgos que esta política trata de reducir son:

- Ataques (internos y externos)
- Errores
- Fraude
- Robo
- Fallos HW y SW

Algunas vulnerabilidades que esta política trata de evitar son:

- Falta de información de los usuarios
- Dificultad en las comunicaciones
- Elección de contraseñas y mantenimiento
- Defectos tecnológicos

5.1 *Activos de nuestros clientes*

Esta política puede ser extendida para incluir activos específicos de nuestros clientes

- Información financiera
- Documentos internos
- Mensajes de Email y mensajería inmediata
- Código fuente del software y paquetes binarios
- Documentación interna de recursos humanos
- Hardware

Algunos proyectos pueden extender y mejorar esta política con requerimientos específicos del cliente..

6 Acceso físico

El objetivo es proteger el acceso físico a la ubicación de las siguientes instalaciones:

- Acceso a las oficinas de Qindel.

Las oficinas de Qindel deben tener acceso limitado para cualquier persona que no sea empleado de Qindel o colaborador. Cada visita debe ser registrada con, al menos, la siguiente documentación:

- Nombre de la persona.
- Hora de entrada
- Hora de salida
- Persona a la que visita
- Acceso a la documentación legal y financiera de Qindel.

Toda la documentación legal o financiera debe tener un control de acceso físico diferente al de la puerta de entrada. (por ejemplo una llave o cualquier otro mecanismo físico). El acceso a esta documentación debe ser limitado

- Centro de cálculo de Qindel.

El acceso físico a los servidores de producción debe estar limitado a las personas del grupo de soporte. Estas instalaciones incluirán al menos:

- panel de conexiones
- Switches de producción
- Routers Internos
- Servidores de producción
- Información del backup de Qindel.

El acceso a la información contenida en el backup, incluidas cintas, discos o utilidades de recuperación de desastres debe ser regulado igual que el acceso al CPD, limitado a las personas del grupo de soporte.

6.1 *Entrada de material al CPD*

En el caso específico del Centro de cálculo de Qindel, hay que regular especialmente qué material puede entrar. En general:

- Se prohíbe la entrada de cualquier material susceptible de provocar o contribuir a la destrucción del CPD (materiales inflamables, como por ejemplo cartón).
- En cualquier caso, todo el material de trabajo que entre al CPD deberá ser inspeccionado por un miembro del departamento IT.
- El departamento IT podrá conceder en último caso y si lo estima estrictamente necesario, el acceso al CPD con cualquier material que se requiera, pero será también responsable de asegurarse de que al abandonar el CPD ningún material peligroso queda en su interior.

7 Acceso Lógico a la infraestructura interna de Qindel

Todas las herramientas de IT en Qindel son aplicaciones internas excepto las siguientes:

- Email
- Dominios públicos de internet (tales como www.qindel.es, www.qindel.com, ...)
- VOIP
- XMPP

7.1 Acceso a las aplicaciones

El acceso a todas las aplicaciones internas puede hacerse por dos vías:

- Desde la red interna en la oficina de Qindel . Este acceso puede hacerse mediante protocolos encriptados o no, si se usan protocolos no encriptados se debe usar un entorno de red conmutado.
- Desde Internet o a través de la red WIFI de Qindel . Todos los accesos externos se deben completar con los siguientes elementos:
 - Autenticación con nombre de usuario / password
 - Un token de seguridad adicional (certificado X.509 u otro)

Esto se puede hacer mediante VPN con certificados más usuario y password (en la VPN o en las propias aplicaciones), o a través de un navegador web con certificado más usuario y password.

7.2 Autenticación de usuarios, autorización y Contabilidad

7.2.1 Autenticación de usuario

Todas las passwords de autenticación de usuario para aplicaciones internas deben ser almacenadas en el servidor de directorio activo interno.

Cualquier excepción a esta regla debe ser autorizada expresamente por el comité de seguridad

El acceso al servidor de directorio activo interno debe estar limitado a un número reducido de administradores, previamente aprobado por el comité de seguridad.

7.2.2 Autorización de usuario

La autorización de los usuarios a las diferentes aplicaciones debe gestionarse preferentemente desde el directorio activo. Si la aplicación tiene varios niveles de acceso, estos deberían ser gestionados mediante grupos de LDAP o roles.

Las excepciones a esta regla deben incluir el procedimiento para gestionar los mecanismos de autorización y los de la cuenta en particular.

7.2.3 Cuentas de usuario

El acceso o intento de autenticación debe quedar registrado y documentado al menos en el registro de logs del directorio activo. Las cuentas de usuario específicas para cada aplicación deben quedar documentadas en los registros de log de cada aplicación.

7.2.4 Política de Contraseñas

Estas son directrices para la política de contraseñas internas:

- Deben expirar periódicamente
- Se deben prohibir las contraseñas con caracteres solo alfabéticos
- La longitud de la contraseña debe ser de al menos 6 caracteres

7.2.5 Creación, actualización y borrado de usuarios

La creación de usuarios debe ser aprobada por el departamento de recursos humanos (para empleados) o por la dirección si son empleados externos.

Las cuentas externas deben tener una fecha de expiración máxima de un año, a menos que se especifique otra cosa.

El borrado de cuentas de usuario debe ser aprobado por recursos humanos (para empleados) o por la dirección si son empleados externos.

Si un usuario (interno o externo) cambia de rol o de proyecto, los nuevos accesos que necesite deben ser aprobados por recursos humanos o por sus superiores y los permisos serán cambiados de acuerdo a esas nuevas necesidades.

7.3 Aplicaciones especiales

Debido a las implicaciones especiales en seguridad que tienen estas aplicaciones, el acceso debería ser específicamente aprobado por el comité de seguridad.

- Administradores de Email.
- Permisos de administrador al servidor de documentación
- Acceso a las aplicaciones de contabilidad y facturación

8 Acceso a Internet

La arquitectura interna de Qindel debería tener al menos los siguientes elementos

- Oficina: Donde se conectan todos los PC's de usuario.
- Red VPN: Se considera con el mismo acceso que la red de oficina.
- Internet: Esta es una red NO segura
- Wireless: Se considera una extensión de Internet
- DMZ: Donde van todas las conexiones de internet y Wireless. En la DMZ no deben estar localizado ningún servicio que contenga datos (bases de datos relacionales, LDAP

server, sistemas de ficheros....)

- Back end: Donde se debe conectar todo el almacenamiento de datos.
- Preproduccion: Redes de laboratorios, que pueden existir opcionalmente.

8.1 Políticas:

- Wireless: en las políticas de firewall de la infraestructura de Qindel se debe considerar como Internet
- La conexión a Internet solo debe ser posible desde la DMZ, y en casos especiales para pruebas de red. Estas conexiones deben estar encriptadas siempre que sea posible
- La VPN se considera con los mismos privilegios que la red de Oficina
- La red DMZ solo debe tener acceso a la red de backend y a Internet, en ningún caso a la red de Oficina. En algunos casos se puede permitir el acceso a la red de Laboratorio.
- En la red DMZ no debe haber nunca almacenamiento de datos
- La red de back end solo tiene acceso a la red DMZ.
- La red VPN y la red de Oficina tienen acceso directo a Internet, DMZ y Back end. A Internet debe accederse a través de un proxy siempre que sea posible.
- La red de preproducción network no tiene acceso a ninguna red en la oficina. Solo la red de Oficina y la VPN tienen acceso a ella.

9 Backup y Recuperación

Todos los elementos de los sistemas de IT deben tener una política de backup y recuperación detallada. Las directrices generales para esto son las siguientes:

- Todos los datos de usuario deben ser copiados diariamente, es decir, en caso de pérdida el usuario debería perder como máximo el trabajo de un día. Se entiende como datos de usuario cualquier cosa que el usuario pueda leer o escribir. Por ejemplo: correo electrónico, datos de facturación y contabilidad, documentos, reportes, sistema de control de versiones, etc.
- Todos los datos de los sistemas deben ser copiados al menos semanalmente. Se entiende por datos de los sistemas el sistema operativo, la configuración de switches y routers y cualquier otro dispositivo de la infraestructura de IT.

9.1 Política de retención

Las políticas de retención debe cumplir con las regulaciones legales. Como mínimo se deben seguir las siguientes directrices:

- El backup diario de los datos de usuario se mantiene durante al menos una semana
- El periodo de retención de los backups semanales debe ser al menos de un mes
- El periodo de retención de los backup mensuales debe ser al menos de 3 meses
- Además se debe mantener un backup semestral y un backup anual

9.2 Política de almacenamiento

El soporte donde se almacene el backup se debe guardar en un lugar seguro, preferentemente en una zona ignífuga. Además se debe guardar un backup semanal en un lugar externo a la oficina.

9.3 Recuperación de desastres

En caso de implementar un sistema de recuperación de desastres la frecuencia en la replicación de los datos no puede ser menor que la frecuencia del backup.

10 Políticas de usuario y requerimientos

10.1 Políticas de usuario

Existen otros documentos relacionados tales como “Qindel End User Security Policy” “Política de control de acceso”, etc que deben ser difundidos entre todos los empleados de qindel y los colaboradores externos. Incluyen al menos:

- En entornos Microsoft es obligatorio el uso de antivirus
- Las actualizaciones automáticas deben estar activadas en los sistemas
- No se deben abrir ficheros adjuntos en un correo de remitente desconocido
- Se debe apagar el equipo o desconectarlo de la red mientras no esté en uso
- Se deben realizar backups de forma regular o almacenar la información relevante en las unidades de disco corporativas.
- Se debe usar un protector de pantalla que necesite ser desbloqueado con usuario y password, y se recomienda que el tiempo de configuración de equipo inactivo para el salvapantallas sea de 5 minutos
- Se recomienda cambiar la password periódicamente y no compartir la password con nadie.
- Mantener el escritorio limpio.
- Mantener las claves y certificados en un lugar seguro..
- El acceso a cualquier equipo como administrador o usuario privilegiado requiere una especial conciencia de seguridad-
- La seguridad es una tarea de todos, cualquier empleado que observe una brecha de seguridad debe comunicarlo a su superior inmediato.

10.2 Equipos de usuario

Se entiende por equipos de usuario cualquier equipo (desktop, laptop, teléfono móvil, tablet, ...) asignado a un empleado específico o colaborador externo y que puede contener datos confidenciales tales como:

- Correos electrónicos
- Documentos Internos de Qindel
- Información interna de clientes de Qindel
- Código fuente interno de Qindel
- Documentos de cliente
- Código fuente interno de clientes
- Cualquier otra información sensible

Cuando el equipo es reasignado a un nuevo empleado o a un nuevo colaborador externo, la información contenida en el dispositivo debe ser eliminada.

Opcionalmente se puede mantener la información en un backup si dicha información se considera sensible o se tienen indicaciones de que debe ser mantenida

Cuando el equipo se desecha, la información contenida en el dispositivo debe ser eliminada.

11 Autores

Nito Martínez <Nito@Qindel.ES>

Juan Antonio Zea Herranz <juan.zea@qindel.com>