ISO 27001

Política de Seguridad

Fecha:	11/03/22
Versión:	v2
Revisión:	1

HISTÓRICO DE REVISIONES

Revisión	Autor	Fecha	Modificaciones respecto a la revisión anterior
2.1	ACN	11/03/2022	Objetivos
2.0	ACN	03/03/2022	Revisión formato. Se elimina el registro de acceso físico de personas ajenas a la oficina
1.9	Juan Zea	12/12/2019	Política de almacenaje en CPD
1.6	Nito Martínez	01/08/2017	Política para equipos obsoletos
1.5	Nito Martínez	15/06/2017	Política de equipos de usuario
1.4	Nito Martínez	10/04/2017	Enhance end user security, reference external document
1.3	Nito Martínez	26/09/2011	End user security
1.1	Nito Martínez		Backups y períodos de retención
1.0	Nito Martínez		Versión Inicial

DOCUMENTOS RELACIONADOS

Título del Documento	Versión / Fecha	Descripción
POSI-04-Politica de Seguridad de Usuario	2.0	
PRO-14-Plan de recuperacion de desastres	1.2	
POSI-07-Politica de control de acceso	1.4	

APROBACIÓN

	Realizado	Aprobado
Nombre:	Nito Martínez	Comite de seguridad
Cargo:	Responable de seguridad	
Fecha:	14/03/2022	

ÍNDICE DE CONTENIDOS

Sumario

1 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.

2 OBJETIVOS

Considerado el propósito básico de este documento establecer los fundamentos generales para la protección de la información y los recursos asociados a las Tecnologías de la Información utilizados, se pretende en concreto:

- Definir la política a seguir en relación con la seguridad de la información.
- Dar directrices para lograr los niveles adecuados de seguridad que permitan una buena gestión de los riesgos identificados.
- Proteger los activos de información conforme a su valor o importancia.
- Preservar la privacidad de clientes, empleados, proveedores y terceras partes.
- Garantizar el cumplimiento de los requerimientos en materia legal.
- Mejorar continuadamente el sistema de seguridad de la información.

3 COMITÉ DE SEGURIDAD

Este comité es responsible 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*"

Información relacionada con este comité puede encontrarse internamente en el REG-23 del SGSI

4 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 TIPOS DE ACTIVOS

- **Activos de información**: Base de Datos de conocimiento, archivos de documentación, manuales, procedimientos..
- **Activos de software**: Software de aplicación, de sistema, herramientas de desarrollo…
- **Activos físicos**: Equipos de comunicaciones, equipos de cómputo, periféricos
- **Servicios**: Servicios de cómputo y comunicaciones, servicios generales (calefacción, A/A, alumbrado..)
- **Personas**: Experiencia y conocimiento del personal contratado
- **Intangibles**: La reputación y la imagen de la organización

5.1 Activos de nuestros clientes

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

- Información financiera
- Documentación técnicas
- Código fuente

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

- Se prohibe 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 neceario, el acceso al CPD con cualquier material que se requiera, pero será también responsible 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
- Dominis 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 mediate 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 comié de seguridad.

7.2.2 Autorización de usuario

La autorización de los usuarios a las diferenctes aplicaciones debe gestionar 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 periodicamente
- Se prohiben las contraseñas con caracteres solo alfabéticos
- La logitud de la contraseña debe ser de al menos 6 caracteres

Información más detallada puede encontrarse en el documento "*POSI-04-Politica de Seguridad de Usuario"*

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 cambmiados de acuerdo a esas nuevas necesidades.

7.3 Aplicaciones especiales

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

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

8 CONEXIÓN DE REDES INTERNAS E 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 Reglas de conexión

- 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 almacenemiento 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 Interne, 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 copiadods 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 escriba. 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.

Mas información puede encontrarse en el documento "*PRO-14-Plan de recuperacion de desastres*"

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 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

10.1 Políticas de usuario

Existen otros documentos relacionados tales como "*POSI-04-Politica de Seguridad de Usuario*" "*POSI-07-Politica de control de acceso*", etc que deben ser difundidos entre todos los empleados de qindel y los colabores 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 límpio.
- 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 expecífico 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 o de Clientes
- Documentos de cliente
- 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>

Alicia Cañas <alicia.canas@qindel.com>