Política de Seguridad Digital
Territoria.

Territoria, compuesto por El Olivar SpA, Territoria SpA, Territoria Asset Management SpA, Territoria Apoquindo S.A., Territoria Santa Rosa SpA, SIR Desarrollo Inmobiliario II SpA y Fondo de Inversión Privado Apoquindo, tiene el compromiso de promover un desarrollo urbano sostenible, creando valor para todos sus grupos de interés. Para lograr este objetivo forman parte del ámbito de su responsabilidad social el respeto irrestricto de los derechos humanos, el cumplimiento íntegro de sus obligaciones laborales, el cuidado del medio ambiente y la construcción de relaciones virtuosas con la comunidad.

Cualquier persona que considere que se haya transgredido alguno de los principios o reglas contenidos en este documento podrá denunciar el hecho de forma confidencial y anónima a cualquiera de los siguientes medios:

- Correo electrónico: mvalles@territoria.cl
- Canal de denuncias: http://denuncias.mut.cl/

Índice

a. Objetivo

La política de Seguridad Digital (en adelante indistintamente "la Política") de Territoria (en adelante también "la Compañía" o "la Empresa") tiene como objetivo proteger a las personas que trabajan en la compañía, proteger los recursos de la compañía, y mantener el orden y la seguridad dentro de la compañía. Esta política contiene un resumen de los principios en uso en Territoria, una lista de los recursos digitales relevantes, convenciones de escritura, y un breve glosario de términos y abreviaturas utilizadas a lo largo del documento.

b. Alcance

El alcance de la Política abarca a toda la actividad de la Compañía, debiendo velar por su cumplimiento en cada uno de sus activos. Esta política es aplicable a todos sus trabajadores, quienes tienen la obligación de denunciar cualquier hecho que pueda constituir una transgresión a los principios o reglas contenidos en ella.

Un recurso digital institucional es todo sitio web, base de datos, directorio digital, listas de correo electrónico, intranets, aplicaciones, o en general cualquier software u objeto digital que pertenece a la compañía, y que es usado y compartido entre dos o más usuarios. Los recursos institucionales digitales que actualmente se encuentran disponibles son los siguientes:

- Correo electrónico institucional: El correo electrónico es el principal mecanismo de comunicación entre funcionarios. Existen dos aplicaciones para acceder al correo electrónico institucional:
  - Microsoft Office 365: Microsoft 365 es nuestra plataforma de productividad con herramientas como Microsoft Teams, Word, Excel, PowerPoint, Outlook, OneDrive y mucho más.
  - Microsoft Outlook: Este es el medio principal y preferente de acceso al correo electrónico institucional. Requiere del uso de un computador provisto por la compañía, y de la instalación del software MS Outlook. Para acceder al correo electrónico a través de este medio se requiere de un nombre de usuario y una contraseña.
- Outlook Web: Este es un medio alternativo de acceso al correo institucional. No requiere de un computador provisto por la compañía; sí se requiere de un browser y de autentificarse a través de nombre de usuario y una contraseña cada vez que se ingresa a la aplicación. Se puede acceder a este recurso en la siguiente URL: http://outlook.com
- Sitios Sharepoint: Sitio web institucional con información diversa. Para acceder a este recurso se requiere de un nombre de usuario y una contraseña.
- BUK: Sitio web institucional con información de remuneraciones, liquidaciones de sueldo, solicitud de vacaciones. Para acceder a este recurso se requiere de un nombre de usuario y una contraseña.
- Softland: Sistema ERP utilizado para la gestión contable, cobranza, financiera y rrhh de la empresa y sus mandantes. Para acceder a este recurso se requiere de un nombre de usuario y una contraseña y la asignación de un perfil de usuario.

- Solutions Malls: Sistema utilizado para la gestión y administración de los contratos de arriendo de los centros comerciales. Para acceder a este recurso se requiere de un nombre de usuario y una contraseña y la asignación de un perfil de usuario.
- Sistema de Ticket: Sistema basado en la plataforma de Zendesk utilizado para la gestión de requerimientos internos.
- Adobe Creative Cloud: Adobe Creative Cloud es un servicio de Adobe que da a los usuarios acceso a los programas de diseño gráfico, edición de video, diseño web y servicios en la nube.
- Autodesk: Suite de programas de diseño.
  - AutoCAD LT. / AutoCAD.
    AutoCAD es un software de diseño asistido por computadora utilizado para dibujo 2D y modelado 3D.
  - Revit. / AutoCAD Revit LT Suite.
    Revit es un software inteligente de diseño y documentación, que permite desarrollar la metodología BIM (Building Information Modeling); facilitando el diseño de los proyectos y los procesos de trabajo en este entorno.
  - BIM Collaborate Pro.
    Autodesk BIM 360 es la plataforma colaborativa en la nube de Autodesk, que permite gestionar y compartir documentos, planos y modelos de proyectos BIM e interactuar con los diferentes actores que intervienen en el ciclo de vida de un proyecto.

Asimismo, la Compañía deberá extender sus obligaciones y exigir su cumplimiento a toda persona con quien suscriba un acto o contrato, cualquiera sea su naturaleza; ya sean proveedores, arrendatarios o cualquier otro. Para lo anterior se establecerán cláusulas que sancionen su incumplimiento, entre las que podrá estar la rescisión del acto o contrato.

Por último, Territoria promoverá su cumplimiento entre las demás partes interesadas, a través de mecanismos de difusión idóneos.

c. <u>Principios</u>

La Compañía ha adoptado los siguientes 4 principios debido a su importancia en relación con el desarrollo de sus actividades y negocios, asumiendo el compromiso de respetarlos y promover su cumplimiento por parte de todos sus grupos de interés.

Para efectos de esta Política, se entiende por grupos de interés a todos aquellos que tienen un interés directo o indirecto en el negocio de Territoria, tales como clientes, trabajadores, arrendatarios, proveedores y contratistas, otras empresas relacionadas o que sostengan relaciones comerciales con la Compañía, comunidad financiera, organizaciones gremiales, medios de comunicación, autoridades, comunidades locales, entre otros.

Principio 1: Uso aceptable de equipos electrónicos.
Describe qué constituye un uso aceptable de los recursos electrónicos institucionales: computadores de escritorio, computadores portátiles (laptops), teléfonos fijos y teléfonos móviles.

Normas generales

- Los equipos provistos por la compañía a cada usuario pueden ser de propiedad de la compañía o mantenerse en arriendo mediante la modalidad de leasing operativo. En ambos casos la compañía es titular de toda la información que se almacena en los equipos provistos por la compañía. la compañía mantendrá un registro de cada una de las personas a las que le son asignados uno o más equipos electrónicos.
- Cada usuario es responsable de proteger físicamente tanto los equipos que se le asignen como la información que en ellos se almacene, en la medida que esta protección no ponga en riesgo su integridad física (por ejemplo, en caso de robo con intimidación o con violencia).
- Cada usuario es responsable de proteger el acceso a cada equipo que se le asigne a través de una contraseña, de acuerdo con lo establecido en la política.
- Cada usuario puede acceder, utilizar o compartir la información de la compañía sólo en la medida que sea necesario para realizar su trabajo.
- Cada usuario tiene la responsabilidad de ejercer el sentido común respecto al uso de los equipos institucionales para actividades personales. En caso de duda, un usuario debe preguntar a su jefe directo, o en su ausencia, al jefe TI.
- Por razones de seguridad, el personal del área informática podrá monitorear remotamente las actividades realizadas por cada usuario a través de los equipos institucionales que le fueron asignados. Este monitoreo en ningún caso tiene por objetivo vigilar las acciones de un usuario, sino detectar software malicioso que pudiera poner en riesgo la información de la compañía o la identidad de los usuarios de la compañía.

En caso de robo, hurto o pérdida de equipos:

En caso de robo, hurto o pérdida de un equipo institucional, el usuario a quien fue entregado el equipo debe reportar el evento dentro de las 6 horas siguientes a que se produzca, o de que se advierta por primera vez su ausencia, incluso si el evento se produce durante horario inhábil.

Todo robo, hurto o pérdida debe ser reportada a través de una de las siguientes opciones:

a) A través del correo electrónico soporte@territoria.zendesk.com

En caso de reportar un robo, hurto o pérdida a través de correo electrónico o de una llamada telefónica, se debe reportar lo siguiente:

a) Nombre del usuario que realiza el reporte o su nombre de usuario.

b) En caso de robo, debe reportarse fecha, hora y lugar del evento.

c) En caso de hurto o pérdida, fecha y hora del momento en que se advirtió por primera vez la falta del equipo, y la fecha y hora estimada del último uso del equipo.

d) Circunstancias en que se produjo el robo o pérdida.

Importante: En caso de robo o hurto de un equipo, es responsabilidad y de carácter obligatorio que el usuario reporte dicho robo a la policía más cercana mediante una constancia, la debe ser entregada al área de TI.

Normas específicas sobre uso de teléfonos móviles

Las normas contenidas en esta sección son aplicables a aquellos usuarios a los que les haya sido asignados teléfonos móviles (smartphones), y deben ser cumplidas en adición a las normas y prohibiciones en el resto de esta política.

1. Los teléfonos móviles (smartphones) provistos por la compañía a algunos usuarios tienen el propósito exclusivo de mantener una línea dedicada de comunicación tanto de voz como de datos con dichos usuarios.

2. Al recibir un teléfono móvil, cada usuario se entenderá en conocimiento tanto la política uso aceptable de equipos electrónicos (pág. 5) como la política uso aceptable de correo electrónico y redes (pág. 8).

3. Las siguientes aplicaciones de comunicaciones podrán ser instaladas en cada teléfono móvil asignado a usuarios de la compañía:

   - WhatsApp, desarrollada por WhatsApp Inc. para mensajes no confidenciales.

4. Si un usuario necesita utilizar una aplicación distinta de las indicadas en el punto anterior, podrá solicitar por escrito al jefe TI que se instale dicha aplicación en su teléfono, justificando la necesidad. El jefe TI podrá autorizar o no la instalación de la aplicación, basado exclusivamente en criterios de seguridad informática. Dicha autorización deberá ser por escrito.

5. Los usuarios que tengan acceso a un correo electrónico a través del teléfono móvil que se les asigne deben seguir estrictamente la política Uso aceptable de correo electrónico y redes (pág.8) para el uso de dicho correo electrónico.

6. Los usuarios que reciban un teléfono provisto por la compañía no deben:

   - Instalar aplicaciones en el teléfono.
   - Desinstalar o modificar aplicaciones ya instaladas en el teléfono.
   - Modificar de cualquier manera la configuración del teléfono.
   - Agregar contactos personales al teléfono, tanto en las aplicaciones identificadas anteriormente, como en la aplicación de contactos nativa del teléfono.
   - Permitir que cualquier otra persona utilice el teléfono, incluyendo familiares y amigos.
   - Reinstalar el sistema operativo del teléfono con privilegios elevados (rooting o jailbreaking), o pedirle a otra persona que lo haga, independientemente de si esta actividad es o no pagada

Prohibiciones

Las actividades en la lista a continuación están en general prohibidas a todos los usuarios de la compañía. Esta lista no pretende ser exhaustiva, sino entregar lineamientos sobre aquellas actividades que son consideradas inadecuadas. Toda excepción debe ser autorizada expresamente por el jefe TI.
Las siguientes actividades están prohibidas para todos los usuarios de la compañía:

Comentado [AO1]: A qué hace referencia? Porque reorganicé todo

Comentado [AO2]: A qué hace referencia? Porque reorganicé todo

1. Bajar o instalar software, plug-ins, add-ons o cualquier otra aplicación propietaria en un equipo electrónico institucional, si el usuario o la compañía no cuenta con la licencia correspondiente.
2. Bajar, instalar, almacenar o reenviar software malicioso, como virus, gusanos, troyanos, bombas de correo electrónico, etc.
3. Conectar cualquier equipo electrónico personal a la red institucional; en específico, está estrictamente prohibido conectar un router inalámbrico o un switch personal a cualquier punto de red de la compañía. En casos justificados, un usuario podrá conectar su computador personal a la red institucional, si cuenta con una autorización previa del Encargado de Seguridad. Para pedir autorización para conectar un equipo electrónico personal a la red institucional, debe pedir autorización a través del correo electrónico: soporte@territoria.zendesk.com.
4. Instalar o ejecutar scripts o programas cuya intención sea interferir con, desactivar o impedir la operación normal de las redes institucionales, o de los equipos institucionales de otros usuarios.
5. Ejecutar cualquier clase de monitoreo de la red institucional que no haya sido autorizada expresa y previamente por el Encargado de Seguridad, a menos que este monitoreo sea parte de las labores habituales del usuario.
6. Instalar cualquier clase de software o aplicación que permita eludir o anular el ingreso de contraseñas para acceder a un equipo institucional.
7. Dispositivos de almacenamiento:
   - Los usuarios no deben utilizar dispositivos de almacenamiento personales, toda información debe ser almacenada en el área de carpetas compartidas dispuesta para esto.
   - No está permitido almacenar información de la empresa en los dispositivos de almacenamiento, solo debe usarse para facilitar el porte de información funcional (ej. presentaciones Power Point).
   - En general la compañía no proveerá de pendrives o discos duros externos o de cualquier medio de almacenamiento externo, por el riesgo que estos representan a la seguridad de la información
   - Todo medio de almacenamiento removible que sea utilizado fuera de la plataforma tecnológica de la empresa debe ser revisado por posible presencia de virus, a través del escaneo de éste por el antivirus instalado en su equipo.

Principio 2: Uso aceptable de correo electrónico institucional y redes.
Este principio describe qué constituye un uso aceptable del correo electrónico institucional y de las redes sociales a través de las redes institucionales; describe también qué constituye un uso aceptable de las redes institucionales y del ancho de banda.

Normas:

I. Uso de correo electrónico institucional

El correo electrónico institucional es provisto a un usuario exclusivamente para comunicarse con el resto de los usuarios, y con personas externas a la compañía cuando su labor así lo requiera.

El correo electrónico institucional no debe ser usado para crear cuentas en redes sociales, sitios de comercio electrónico, tiendas de comercio, o en general cualquier clase de servicio provisto en línea, excepto si este servicio está directamente relacionado con la labor del usuario.

Por razones de seguridad, el correo electrónico institucional es revisado por programas automáticos para filtrar virus, malware, spam, y otros tipos de amenazas que se esparcen a través del correo electrónico. A pesar de que el correo electrónico institucional no será leído o revisado por seres humanos, los mensajes de los usuarios pueden ser revisados por filtros automáticos y ser marcados para ser revisados posteriormente por personal del área informática en caso de que el contenido del mensaje calce con criterios predefinidos de riesgo.

En ningún caso, el usuario se encuentra autorizado a modificar el texto de su firma de correo, ni su fuente, ni su tamaño. Como tampoco agregar ningún tipo de imagen o sticker. Todo cambio de cargo en la firma de correo lo realizará TI una vez notificado por el departamento de personas y DO o su jefatura directa.

II. Uso de Internet y redes sociales

Un usuario puede navegar normalmente por Internet a través de las redes institucionales, ejerciendo su buen juicio para decidir qué sitios visita, y siendo austero en términos del ancho de banda que utiliza. En este sentido, se recomienda lo siguiente:
a) Está permitido escuchar música a través de Internet, siempre y cuando se realice con sistema de audífonos personales.
b) Evitar reproducir películas a través de Internet; por ejemplo, a través de servicios como Netflix o YouTube.

Por razones de seguridad, todos los sitios que un usuario visita podrían ser monitoreados por filtros automáticos, y algunos sitios pueden ser marcados por filtros automáticos para ser revisados por personal del área informática.

El área informática puede bloquear parcial o completamente sitios web o direcciones en Internet cuando:
a) Estas direcciones se encuentren en listas negras de cualquier tipo. El área informática podrá publicar una lista de aquellas listas negras que utiliza para bloquear sitios web.
b) Estas direcciones contengan pornografía, o contenido difamatorio o denigrante para cualquier persona; o contenido racista o discriminador de cualquier especie.
c) Uno o los gerentes generales así lo solicite(n) bajo razones fundadas.

Un usuario puede hacer uso de sus cuentas personales de redes sociales o de su correo electrónico personal a través de las redes institucionales, siempre y cuando:
a) Este uso no lo distraiga de sus labores habituales.

b) No revele información relacionada con su trabajo o el trabajo realizado por otros usuarios de la compañía.
c) Sus mensajes no sean difamatorios, denigrantes, racistas, o discriminadores para con cualquier otro usuario de la compañía, o para personas externas a la compañía.
d) No haga uso excesivo del ancho de banda puesto a disposición de los usuarios de la compañía. El qué constituye un uso excesivo será analizado caso a caso por el área informática; en caso de duda, un usuario debe preguntar al jefe TI.

III. Representación de la compañía

Todo mensaje de un usuario de la compañía a través de redes sociales es de su exclusiva responsabilidad, y no compromete de manera alguna la posición o parecer de la compañía, ni de sus representantes.

Ningún usuario está autorizado para enviar mensajes a través de redes sociales en nombre de la compañía, a excepción de las más altas autoridades (Gerentes) y quienes ellas autoricen expresamente.

IV. Prohibiciones

Las siguientes actividades están prohibidas para todos los usuarios de la compañía. Toda excepción debe ser autorizada expresamente por el Encargado de Seguridad. Está estrictamente prohibido:

1. Utilizar el correo electrónico institucional para crear cuentas en servicios de apuestas en línea, sitios pornográficos, sitios de citas o de búsqueda de pareja, o cualquier otro sitio cuyo uso vaya en contra de las normativas de la empresa.
2. Utilizar las redes institucionales para bajar, almacenar, distribuir, reenviar o transmitir cualquier material que infrinja la Ley 17.336 sobre Propiedad Intelectual y Derecho de Autor; por ejemplo, música, películas, series de televisión, aplicaciones, libros, imágenes, fotografías, etc.
3. Utilizar las redes institucionales para bajar, almacenar, distribuir o reenviar cualquier tipo de material pornográfico, ya sea a través de imágenes, audio, o video.
4. Utilizar el correo electrónico institucional o las redes institucionales para vender productos u ofrecer servicios de cualquier naturaleza.
5. Utilizar el correo electrónico institucional para enviar correo electrónico no solicitado (spam).
6. Utilizar el correo electrónico institucional o las redes institucionales para enviar mensajes para acosar o molestar sexualmente a otras personas, pertenezcan éstas o no a la institución.
7. Modificar las firmas de correo electrónico, ya que estas deben ser autorizadas por su jefatura y RRHH.

Principio 3: Uso de contraseñas.
La selección y uso de buenos contraseñas constituye una parte importante de la seguridad de una institución. Un "buena contraseña" es aquel que es fácil de recordar por su titular, difícil de adivinar por otras personas, y difícil de averiguar a través de medios automáticos. Una mala contraseña puede ser adivinado por otras personas, y puede permitir a esas personas tener acceso a recursos a los que no debería tener acceso. Todos los usuarios somos responsables de escoger buenos contraseñas para los recursos digitales institucionales a los que se nos provee acceso.

Normas:

I. Creación de accesos y perfiles

Al ingresar un nuevo colaborador a la compañía se le asignará un nombre de usuario y rol en función de lo indicado en el Check list de Software y Aplicaciones para Estaciones de Trabajo", en la que se establecen los requerimientos técnicos que requerirá el candidato elegido para desarrollar sus funciones, tales como computador, software, mail, intranet, accesos, entre otros, y deberá entregar directamente al área de TI para su gestión, con firma autorizada de la gerencia interesada. Será la gerencia interesada la responsable de hacer seguimiento del cumplimiento de este proceso directamente con el área de TI, sin intermediación RRHH para este propósito la idea es que cuando el nuevo colaborador ingrese a trabajar cuente con toda la implementación ´necesaria para poder desarrollar su labor.

II. Cambios o ampliación de perfil

Un cambio o ampliación de perfil debe ser solicitado a TI por RRHH, cuando corresponde a un cambio de área del colaborador.
Cuando por necesidad se requiera una ampliación temporal de un usuario, esta solicitud debe realizarla el jefe directo del área y notificado vía correo electrónico a TI indicando claramente las nuevas atribuciones y por cuanto tiempo serán aplicadas.

III. Creación de contraseñas

1. Todos los recursos digitales institucionales deberán ser protegidos a través de una contraseña. Toda contraseña debe ser creado siguiendo lo establecido en las recomendaciones para el mundo digital (pag.18).

2. A veces, por razones de buen servicio, a un usuario se le asigna una contraseña provisional que es comunicado verbalmente o que es entregado por escrito en una hoja de papel. Todo usuario al que se le asigna una contraseña provisional deberá cambiar esta contraseña la primera vez que ingrese al recurso digital correspondiente.

IV. Protección de contraseñas

1. Una contraseña siempre es de uso personal. Un usuario no debe revelar ni compartir ninguno de sus contraseñas con otros usuarios, incluyendo asistentes, secretarios, administradores, y familiares del usuario. Esto es aplicable especialmente cuando un equipo electrónico institucional sea usado en el hogar del usuario, o cuando el usuario está de vacaciones, con permiso o fuera de su puesto de trabajo.
2. Una contraseña no debe ser compartido ni revelado bajo ninguna circunstancia a personas externas a la compañía, incluyendo familiares del usuario o personas que vivan bajo el mismo techo que el usuario.
3. Una contraseña debe ser único; es decir, no debe ser reutilizado en ningún otro recurso institucional digital.
4. Una contraseña no debe ser almacenado en medios físicos o digitales, tales como archivos de texto sin encriptar, pendrives USB, discos duros externos, CDs o DVDs. En particular, un usuario no debe utilizar la funcionalidad de almacenamiento de contraseñas ofrecida por los browsers.
5. Una contraseña no debe ser enviado ni comunicado oralmente, a través del teléfono, correo físico, memorándums, oficios, circulares, correo electrónico, mensajes de texto (SMS), fotos, imágenes, o cualquier otro medio físico o digital.
6. Una contraseña no debe ser escrito ni guardado en ninguna parte de la oficina de un funcionario.
7. El que una persona averigüe la contraseña de un usuario a través de cualquier método constituye un acceso no autorizado a los recursos digitales institucionales. Todo usuario que sospeche que una de sus contraseñas pueda haber sido averiguado o espiado por otras personas deberá:
   - cambiar inmediatamente su contraseña.
   - reportar el incidente inmediatamente al jefe TI. Para reportar el incidente, el usuario debe seguir el procedimiento establecido en la política Respuesta a Incidentes de Seguridad Digital (pág. 20).

V. Delegación de identidad

En caso de que un funcionario/a, por la naturaleza de su cargo, deba delegar parte de la administración de su identidad a otros funcionarios/as, deberá solicitar apoyo al área informática para poder realizar estas acciones sin que tenga que revelar su contraseña a otras personas.

Principio 4: Respuesta a incidentes de seguridad digital.

Cualquier persona dentro de una institución puede hoy sufrir un incidente de seguridad digital. La mayor parte de las políticas y guías de buenas prácticas de la compañía están dedicadas a prevenir la ocurrencia de incidentes de seguridad digital. Sin embargo, es fundamental que en caso de que ocurra un incidente, la o las personas que sepan del incidente sean capaces de reconocerlo y reportarlo, para que entre todos seamos capaces de remediar las consecuencias del incidente

Normas:

I. Prevenir incidentes

Todo usuario debe conocer y practicar lo contenido en las recomendaciones para el mundo digital (pag. 13), con el objetivo de prevenir ataques digitales sobre los equipos electrónicos que le son asignados y sobre los recursos digitales institucionales a los que tiene acceso.

II. Identificar incidentes

Todo usuario debe conocer lo contenido en la Guía de Identificación de Incidentes de Seguridad, con el objetivo de saber identificar los incidentes de seguridad allí descritos.

III. Remediar incidentes

Todo usuario que ha identificado un incidente de seguridad en un equipo electrónico a su cargo debe seguir el siguiente procedimiento:

Si se trata de un computador de escritorio o computador portátil:

1. Si el computador está conectado a la red, desenchufe inmediatamente el cable de red. No apague el computador.
2. Si tiene acceso inmediato a Internet a través de otro computador, abra la siguiente URL: Formulario
   y siga las instrucciones que allí se indican para reportar el incidente en la intranet corporativa en la sección TI.
3. Si no tiene acceso inmediato a Internet, comuníquese inmediatamente con el Jefe TI al teléfono +569 9144 1400 para reportar el incidente.
4. Si no tiene acceso inmediato ni a Internet ni acceso a un teléfono, consiga un computador con conexión a Internet o un teléfono lo más pronto posible para reportar el incidente.

d. **Recomendaciones para el mundo digital**

Este capítulo presenta 7 recomendaciones para el mundo digital institucional y personal. Estas recomendaciones van dirigidas a los colaboradores de la compañía que deben tener especial cuidado en proteger su información y la información de la compañía donde trabajan; sin embargo, este capítulo debería ser útil para todas las personas que quieran tomar medidas básicas de seguridad digital.

1. Cuida tus contraseñas.

La contraseña es hoy el mecanismo más utilizado para acceder a servicios de acceso restringido. A pesar de que ha habido muchas propuestas alternativas, es muy poco probable que los contraseñas lleguen a ser reemplazados en el futuro cercano.

Una buena contraseña es aquella que es fácil de recordar para la persona que lo creó, y difícil de adivinar o averiguar para cualquier otra persona. Lamentablemente, esto es difícil de hacer porque

los contraseñas más seguras son cadenas de caracteres escogidos aleatoriamente, y éstos son muy difíciles de recordar. Incluso cuando los escribimos, estas contraseñas son tan difíciles de ingresar en un teclado o la pantalla de un teléfono inteligente, que usualmente terminamos renunciando a contraseñas seguros y usamos contraseñas que en vez de eso son fáciles de recordar y de ingresar en cualquier parte (como "123456").

Algunas recomendaciones para cuidar tus contraseñas:

- **Recomendación 1:** Usa contraseñas distintas para cada identidad digital (ej. Laboral o Personal). Según un estudio del año 2007, las personas tenemos en promedio 25 cuentas o sitios que requieren de una contraseña, y tenemos en promedio 6.5 contraseñas distintos [7]. Esto significa que, en promedio, reusamos la misma contraseña en alrededor de 4 sitios.
- **Recomendación 2:** Usa contraseñas largos y difíciles de adivinar por otras personas. En general, los contraseñas más largas son más seguros para la mayor parte de los propósitos cotidianos.

2. Bloquea tu computador/teléfono.

Frente a los problemas anteriores, una forma sencilla de evitar el problema tanto con smartphones como con computadores es bloquearlos para impedir que otros tengan acceso a éste. Todos los computadores, laptops, tablets, y smartphones modernos ofrecen opciones para bloquearlos y evitar que otras personas tengan acceso a nuestros aparatos. En los computadores con Microsoft Windows, se puede bloquear el computador presionando las teclas "Windows" y "L" (de "lock"); para desbloquear se utiliza la combinación CONTROL + ALT + SUPRIMIR, y luego se ingresa la misma contraseña del usuario que bloqueó el computador. En los computadores con iOS (Mac) existen mecanismos similares para bloquear el computador.

- **Recomendación 3:** Bloquea tu teléfono por lo menos con un número de al menos cuatro dígitos.
- **Recomendación 4:** Bloquea tu computador siempre que te ausentes por más de unos segundos.

Esto es especialmente recomendable para el lugar de trabajo, donde otras personas pueden sentarse y tener acceso a mi computador (no sólo colegas de trabajo sino también personas que no pertenecen a la institución).

3. Seguridad en Redes de datos

a) No te conectes a redes inalámbrica que no conozcas.

Cuando te conectas a una red inalámbrica (Wifi), todo tu tráfico pasa a través de un pequeño computador especializado conocido como router. Este computador, además de conectarte a Internet (técnicamente, a un proveedor de servicios de Internet o ISP, como Claro, Entel, WOM, etc.), es responsable principalmente de mostrarte los sitios correctos. Este computador está siempre bajo control de alguien; y esa persona, empresa o institución pública puede decidir (si así lo desea) restringir tu navegación de casi cualquier forma imaginable:

* Puede mostrarte otros sitios en vez de los que tú quieres visitar,
* Puede silenciosamente censurar ciertos sitios para que no los visites, o facilitar la visita a ciertos sitios específicos,
* Puede espiar tu tráfico y mostrarte cosas basado en ese tráfico,

* Etc.

En la práctica, la confianza que uno puede tener en una red inalámbrica es la misma confianza que uno deposita en la persona, empresa o institución que controla el router. Por tanto, las principales recomendaciones sobre esto son las siguientes:

- **Recomendación 5:** Antes de conectarte a una red inalámbrica, confirma con alguna persona que pertenezca a la institución cuál es el nombre de la red.

Por ejemplo, si sueles tomarte un café en la tienda de la esquina, pregunta a las personas que te atienden en el café cuál es el nombre de la red antes de conectarte. Tiendas como Starbucks cambian cada cierto tiempo el nombre de la red en cada local.

b) No abras correos o archivos de personas que no conoces

El correo electrónico es (y seguirá siendo durante un buen tiempo) una herramienta de comunicación importante dentro de las instituciones. Uno de los problemas más complejos de esta herramienta, sin embargo, es que requiere poco conocimiento el hacerse pasar por otra persona, y el enviar correos masivos con el propósito de engañar a otros, o de infectar sus computadores con malware (a través de archivos adjuntos).

Es por esto que una de las principales recomendaciones es la siguiente:

- **Recomendación 6**: No abras correo electrónico de personas o instituciones que no conoces.

A pesar de que esto no es suficiente, en general es un muy buen hábito el no responder (y simplemente eliminar) los correos de personas o instituciones que no conocemos. ¿Cómo hacemos para recibir correos de personas que conocemos, pero de las cuales no hemos recibido correo antes? Para eso, siempre deberíamos primero chequear físicamente con la persona su correo electrónico.

- **Recomendación 7:** Siempre chequea las peticiones extraordinarias con la(s) persona(s) involucradas.

¿Cuáles son las posibilidades de que, a nuestro mejor amigo, al que no vemos hace un par de meses, le hayan robado todo mientras paseaba por Ucrania, que haya perdido su pasaporte y su dinero, y necesite que le prestes $2.100 euros para pagar la cuenta del hotel?

La respuesta es: depende de si es o no razonable que la persona en cuestión esté viajando por Ucrania. Este es un engaño tradicional a través de correo electrónico, y lo más probable es que algún hacker haya tomado el control de la cuenta de correo electrónico de nuestro amigo, y esté enviando correos pidiendo dinero a toda la lista de contactos de nuestro amigo. En cualquier caso, lo mejor que uno puede hacer es sencillamente llamar a la persona por teléfono, o ubicarla de alguna otra forma para confirmar la veracidad del problema.

e. Implementación

Este documento debe ser implementado de conformidad con la legislación vigente, las regulaciones y las normas nacionales, así como las existentes en el país donde se encuentre cada activo y las normas internacionales, según corresponda. Para estos efectos deberá considerarse toda disposición

relacionada con la normativa vigente en materia laboral, medio ambiental, no discriminación e inclusión, entre otras.

En caso de existir conflicto entre los principios y reglas definidos en la presente Política y cualquiera de esas normativas, prevalecerá siempre lo dispuesto por estas últimas.

El monitoreo y control del cumplimiento de la Política le corresponderá al área responsable.

El responsable de la Política dará cuenta al Equipo Ejecutivo o Comité respectivo de forma anual sobre el avance en la implementación, así como de las situaciones de incumplimiento detectadas y de las medidas correctivas adoptadas en consecuencia.

Los planes, procedimientos y/o acciones de implementación o mejora serán dados a conocer de forma periódica por la Empresa a sus grupos de interés por medios idóneos.

f. Quejas y reclamos

Cualquier persona que considere que se haya transgredido alguno de los principios o reglas contenidos en este documento podrá denunciar el hecho de forma confidencial y anónima a cualquiera de los siguientes medios:

- Correo electrónico: misdatos@territoria.cl
- Canal de denuncias: http://denuncias.mut.cl/

Comentado [AO3]: CREAR CORREO

Las denuncias serán conocidas por el Encargado de Prevención del Delito, cuando este sea nominado, quien implementará el procedimiento establecido en el Código de Ética y Conducta de la Empresa, resguardando el anonimato y confidencialidad del denunciante, así como los principios y reglas del debido proceso.

g. Revisión

La Política será revisada periódicamente para asegurar su adecuación y efectiva implementación. Todas las revisiones estarán sujetas a la aprobación del Equipo Ejecutivo o Comité respectivo.

h. Difusión

Será responsabilidad del Gerente General tomar todas las medidas que estime conveniente para dar a conocer la Política y capacitar respecto de ella a los distintos grupos de interés, con especial preocupación por los trabajadores de la Empresa, arrendatarios, proveedores y sus respectivos trabajadores.

La difusión de contenidos asociados a esta política deberá asegurar que se realice de forma no discriminatorias y respetuosas de las diferentes culturas, sin afectar negativamente a los públicos más vulnerables, como los niños, los adultos mayores y población extranjera.

Además, los contratos y comunicaciones deberán ser claros y sencillos, redactados en un lenguaje lo más cercano posible al utilizado normalmente por las personas a las que se dirige el mensaje; deberá acatar la legislación estatutaria, sin recurrir a prácticas evasivas o indebidas; ser exhaustivo y no omitir ningún elemento relevante que pueda afectar la decisión, estando disponible en los sitios web de la Compañía y estableciendo mecanismos para responder a las necesidades de las personas con discapacidad.

i. Vigencia

Esta política entró en vigencia desde que fue aprobada, no habiendo sido modificada a la fecha.

j. Glosario

Glosario

Browser o navegador: Software que permite visualizar páginas web. Existen muchas marcas distintas de browsers: los más conocidos son Chrome y Chromium (de Google), Firefox (de Fundación Mozilla), Opera (de Fundación Opera), y Safari (de Apple). El browser Internet Explorer (de Microsoft) está siendo discontinuado, y su uso no se recomienda. En su reemplazo utilizar EDGE del mismo fabricante.

Contactos personales: Respecto de un usuario de la compañía, se refiere a datos de contacto de personas que no tienen una relación laboral con el usuario.

Cuentas personales: Todas aquellas cuentas de correo electrónico o redes sociales que pertenecen a un usuario de la compañía, pero que son de uso privado e individual, y que no son controlados ni provistos por la compañía.

Correo electrónico institucional: Cuenta de correo electrónico asignada a un usuario de la compañía y administrada por ésta. Las direcciones de correo electrónico institucional siempre tienen la forma de nombredeusuario@territoria.cl; por ejemplo, si el usuario "Juan Pérez" posee el nombre de usuario jperez, su correo electrónico institucional será jperez@territoria.cl.

Correo electrónico personal: Toda cuenta de correo electrónico que pertenece a un usuario de la compañía, pero que es provista por un proveedor externo, no contratado por la compañía; p.ej., Gmail, Yahoo, etc.

Equipo electrónico institucional o Equipo institucional: Cualquier aparato electrónico que sea propiedad de la compañía, y que es temporalmente puesto a disposición de un usuario para ayudarlo a cumplir con su labor. Por ejemplo, un computador de escritorio, un computador portátil, un teléfono móvil (smarphone), un teléfono fijo, una impresora, un router, un switch, etc.

Equipo electrónico personal: Aquel aparato electrónico que no le sea asignado a un usuario de la compañía.

Área TI: Grupo de personas que proveen servicios de apoyo a funcionarios de la compañía en las siguientes actividades:

- Facilitar el desarrollo, implementación y explotación de proyectos tecnológicos.
- Instalación y soporte de equipos electrónicos institucionales, junto con la conexión a redes de estos equipos.

- Instalación y administración de aplicaciones y programas en los equipos anteriores.

Horario hábil: lunes a viernes, de 09:00 a 18:00 horas, exceptuando días feriados.

Horario inhábil: Cualquier instante que queda fuera de la definición de horario hábil.

Incidente de seguridad: Cualquier evento que involucre equipos o redes institucionales, y que contravenga alguna de las normas de la compañía.

Listas negras (blacklists): Listas públicas de nombres de dominios, URLs o direcciones IP que han sido reportados por distribuir malware o por enviar correo electrónico no deseado (spam). Estas listas usualmente son administradas por empresas de seguridad o grandes corporaciones (p.ej., Google, Apple) para proteger a los usuarios que hacen uso de sus productos o servicios.

Contraseña provisional: Aquella contraseña que es asignado de manera temporal para acceder por primera vez a un servicio o recurso digital institucional. Usualmente, una contraseña provisional es comunicado al titular ya sea verbalmente o por escrito.

Recurso digital institucional: Todo sitio web, base de datos, directorio digital, listas de correo electrónico, intranets, aplicaciones, o en general cualquier software u objeto digital que pertenece o se mantenga en modalidad de arriendo a la compañía, y que es usado y compartido entre dos o más usuarios.

Redes sociales: Facebook, Twitter, LinkedIn, Instagram, Pinterest, Tiktok y en general cualquier otro servicio de comunicación masiva en Internet.

Redes institucionales: Todas aquellas redes y equipos de comunicaciones de propiedad de la compañía, que sean utilizados para comunicar a dos o más usuarios entre sí y a Internet. Esta denominación incluye cables de red, puntos de red, routers, switches, firewalls, ISP, y en general cualquier otro equipo de comunicaciones en uso en instalaciones de la compañía o de los centros comerciales que administra.

Nombre de usuario: Nombre de usuario utilizado para identificar a un usuario de manera única.

Usuario o colaborador: Cualquier persona que trabaja para la compañía, independientemente del tipo de vinculación laboral que mantenga con la institución. En este documento ambos términos se usan indistintamente.

Perfil de Usuario: Conjunto de atributos asignados a un nombre de usuario para su desempeño en los recursos digitales institucionales, este perfil de usuario está directamente establecido desde la descripción de cargo del usuario.