



Online **Payslip** Service

ROSCLAR

Política de Seguridad

Portal del empleado

Tabla de contenido

Contenido

Objeto del documento.....	3
Objetivo de la seguridad	3
Seguridad.....	3
Protección física del servicio	3
Protección lógica del servicio	4
Seguridad ligada a los recursos humanos.....	5
Política de credenciales de acceso a aplicación	5
Acceso HTTPS/SSL	5
Generación de contraseñas y su gestión	6
Prueba del proceso de creación de contraseñas aleatorias	7
Prueba de la política de contraseñas implementada	8
Prueba de la política de bloqueo de cuentas de usuario.	9
Prueba que las contraseñas se guardan hasheadas en base de datos	10
Prueba de la política de sesiones inactivas	10
Política de backup de los datos de nuestros clientes	10
Gestión de comunicaciones y operaciones	11
Plan de continuidad de negocio	12
Certificaciones de seguridad y valor añadido	12
Cumplimiento legal	12

Objeto del documento

El presente documento tiene por objeto establecer la Política de Seguridad de la Información de Rosclar en relación al servicio prestado por Rosclar acerca de la aplicación a3HRgo, basada en los requisitos dispuestos en el estándar ISO/IEC 27001:2013.

Objetivo de la seguridad

Tiene por objetivo asegurar que todos los tratamientos de información relativos a los procesos de negocio indicados en el alcance se realizan de forma segura y únicamente por personal autorizado.

De esta forma se garantizan la confidencialidad, la integridad y la disponibilidad de la información de los clientes de Rosclar.

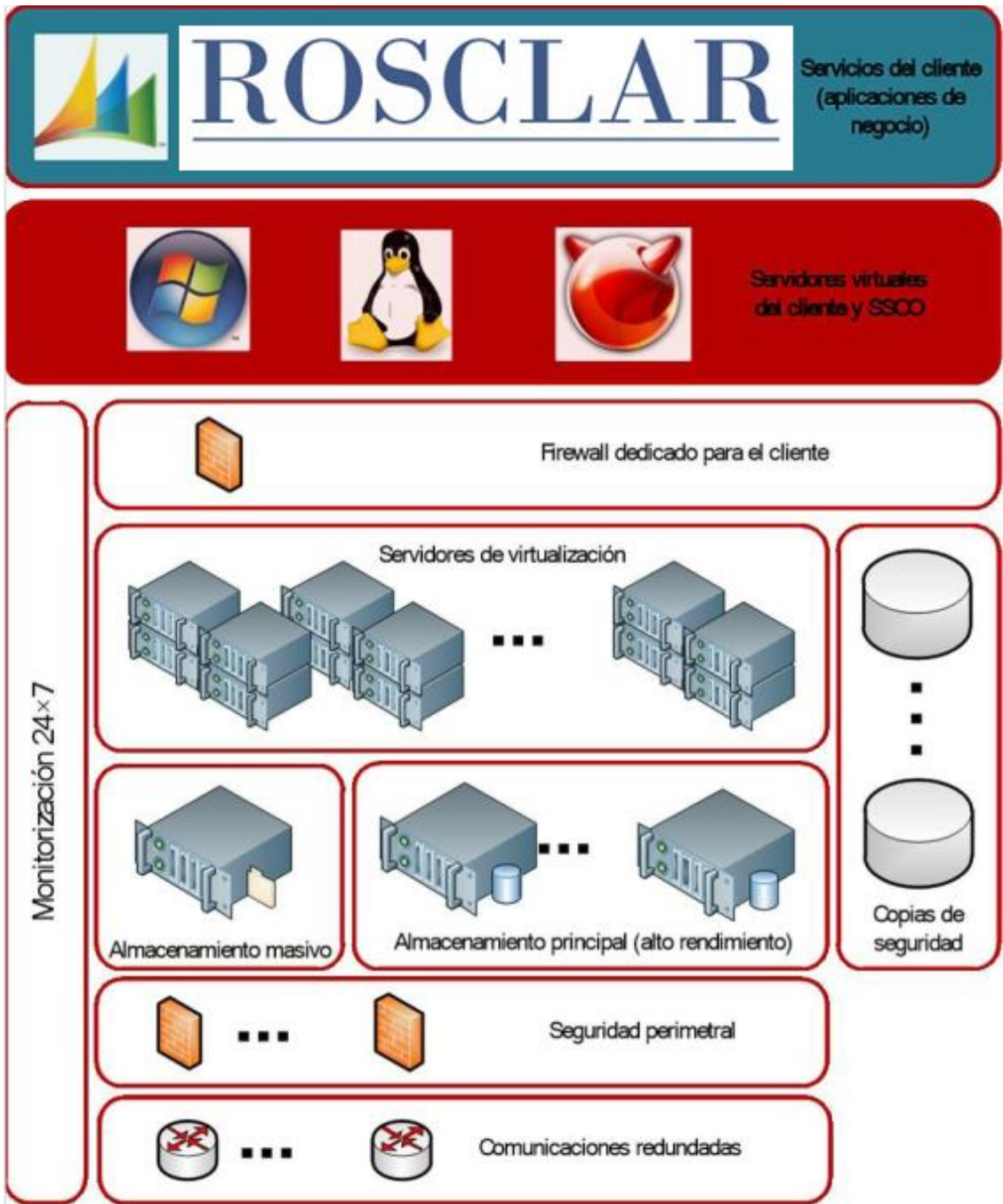
Seguridad

Protección física del servicio

Los elementos físicos esenciales para ofrecer el servicio, como son los servidores físicos o los sistemas de almacenamiento principales, se encuentran **redundados** y configurados en **alta disponibilidad**, según sea adecuado dada su naturaleza. Se dispone de recursos suficientes para que los fallos simples en elementos hardware no afecten de forma significativa al servicio mientras las anomalías estén presentes.

La infraestructura física para alojar el servicio IaaS de Rosclar se encuentra alojada en centros de datos que ofrecen las características necesarias para **asegurar**:

- la temperatura correcta de los distintos elementos hardware;
- la humedad adecuada del ambiente;
- la disposición de un ambiente libre de elementos contaminantes como polvo en suspensión;
- la disponibilidad de energía de forma ininterrumpida, incluso en caso de fallo del suministro eléctrico principal;
- la redundancia de las comunicaciones con operadores diferentes;
- la protección adecuada ante eventos que puedan causar daño a las infraestructuras, como incendios;
- la seguridad física necesaria en los edificios, las salas, los pasillos y los armarios, con controles de acceso **24x7**.



Protección lógica del servicio

Se previene el acceso no autorizado a los sistemas operativos, y se requiere su actualización para corregir vulnerabilidades detectadas; se proveerán de las medidas técnicas de seguridad oportunas.

Estará restringido y controlado el uso de aplicaciones no autorizadas que puedan invalidar las medidas de seguridad implantadas.

Seguridad ligada a los recursos humanos

Se asegura que todos los empleados, contratistas y los terceros entienden sus responsabilidades y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos puestos a su disposición.

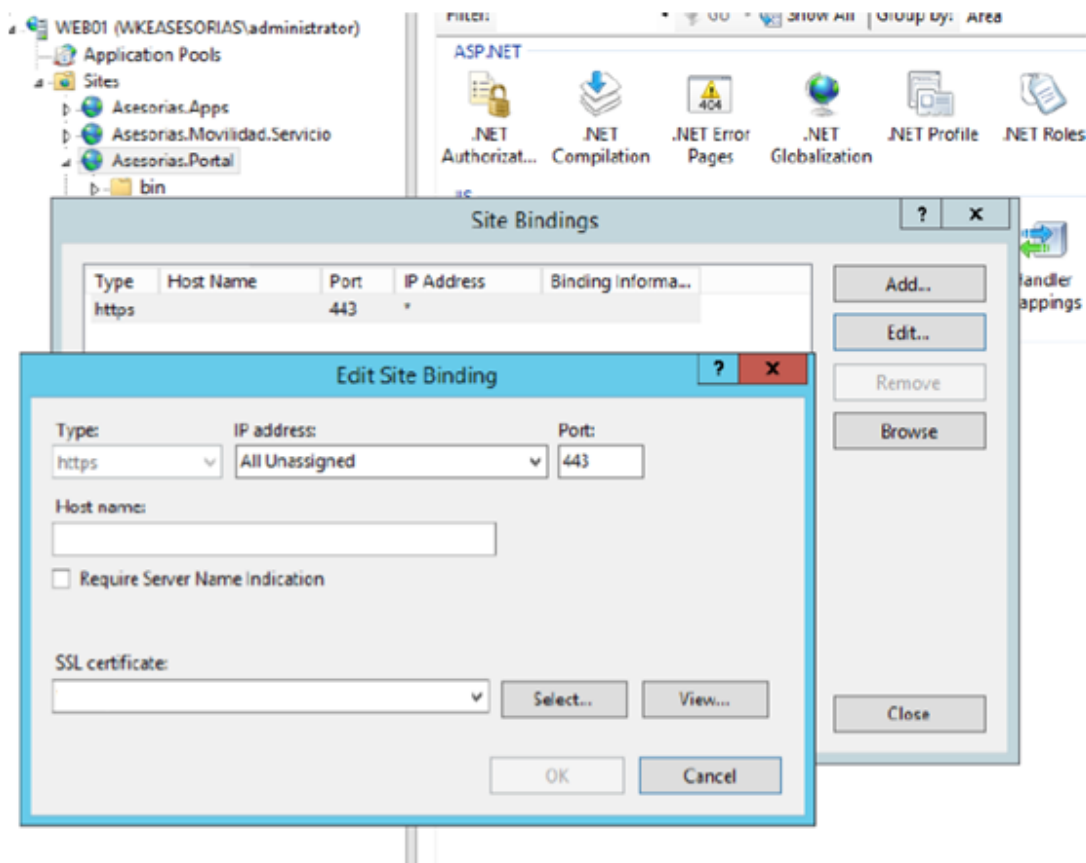
Se asegura que todos los empleados, contratistas y los terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano. Se asegura que todos los empleados, contratistas y los terceros abandonan la organización o cambian de puesto de trabajo de forma ordenada y sin comprometer la seguridad de la misma.

Política de credenciales de acceso a aplicación

A continuación se muestran una serie de pruebas de todos los pasos que afectan a la política de credenciales de acceso, que sea segura, que las contraseñas tengan la complejidad requerida, y todo lo relativo a bloqueo de cuentas y sesiones inactivas.

Acceso HTTPS/SSL

En la imagen se puede ver la configuración relativa a los protocolos seguros HTTPS y SSL que tienen los servidores.



Generación de contraseñas y su gestión

La emisión de contraseñas automáticas genera una contraseña de 10 caracteres siguiendo el siguiente patrón:

- Utiliza el método de .NET System.Web.Security.Membership.GeneratePassword ([https://msdn.microsoft.com/es-es/library/system.web.security.membership.generatepassword\(v=vs.110\).aspx](https://msdn.microsoft.com/es-es/library/system.web.security.membership.generatepassword(v=vs.110).aspx)) pasando como parámetros 7 y 1 (7 caracteres de contraseña y al menos un carácter no alfanumérico)
- Sustituye el carácter no alfanumérico generado por el carácter '@' (Regex.Replace(result, "[^0-9a-zA-Z]+", "@"))
- Añade al final '7wX' (para forzar que haya siempre un número, una letra minúscula y una letra mayúscula).

Prueba del proceso de creación de contraseñas aleatorias

En la imagen se muestra el código que genera las contraseñas aleatorias tal y como se han descrito.

```
public static string GeneratePassword()
{
    string result = string.Empty;

    result = System.Web.Security.Membership.GeneratePassword(7, 0);
    result = Regex.Replace(result, "[^0-9a-zA-Z]+", "@");
    result += "7wX";

    return result;
}
```

Y una muestra del email que se envía:



vi. 01/07/2016 10:20
provision@a3hrgo.com
Bienvenido a A3HRgo!

Para [redacted]

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Acceso a la Solución

Accede directamente a tu cuenta de a3HRgo:

Entrar a Rosclar - Portal del Empleado

Introduzca el siguiente usuario y contraseña (podrá cambiar estos datos una vez esté dentro del programa).

Usuario: [redacted] Password: VD@vW@c7wX

Servicios disponibles

Le Informamos de los servicios que tiene a su disposición para trabajar con la aplicación y que le ayudarán en el día a día a resolver sus dudas.

Servicio Posventa:

Desde el icono , situado en la parte superior derecha de la aplicación, podrá realizar consultas o comunicar algún error a nuestro Departamento de Posventa.

Sistema de Ayudas:

Prueba de la política de contraseñas implementada

En la imagen se muestra el código que rige la política de complejidad de las contraseñas

```
public static ApplicationUserManager Create()
{
    var manager = new ApplicationUserManager(new UserStore<ApplicationUser>(ApplicationDbContext.Create()));
    // Configure validation logic for usernames
    manager.UserValidator = new UserValidator<ApplicationUser>(manager)
    {
        AllowOnlyAlphanumericUserNames = false,
        RequireUniqueEmail = true
    };
    manager.UserLockoutEnabledByDefault = true;
    manager.DefaultAccountLockoutTimeSpan = new TimeSpan(0, 20, 0);
    manager.MaxFailedAccessAttemptsBeforeLockout = 5;
    // Configure validation logic for passwords
    manager.PasswordValidator = new PasswordValidator
    {
        RequiredLength = 6,
        RequireNonLetterOrDigit = false,
        RequireDigit = true,
        RequireLowercase = true,
        RequireUppercase = true,
    };
    // Register two factor authentication providers. This application uses Phone and Emails as a step of receiving a
    // You can write your own provider and plug in here.
    manager.RegisterTwoFactorProvider("PhoneCode", new PhoneNumberTokenProvider<ApplicationUser>
    {
        MessageFormat = "Your security code is: {0}"
    });
    manager.RegisterTwoFactorProvider("EmailCode", new EmailTokenProvider<ApplicationUser>
    {
        Subject = "Security Code",
        BodyFormat = "Your security code is: {0}"
    });
    manager.EmailService = new EmailService();
    manager.SmsService = new SmsService();

    return manager;
}
```


Prueba de la política de bloqueo de cuentas de usuario.

En la imagen se muestra el código que implementa el bloqueo de cuentas y el tiempo necesario de inactividad para ejecutarlo. 1 0

```
public static ApplicationUserManager Create()
{
    var manager = new ApplicationUserManager(new UserStore<ApplicationUser>(ApplicationDbContext.Create
    // Configure validation logic for usernames
    manager.UserValidator = new UserValidator<ApplicationUser>(manager)
    {
        AllowOnlyAlphanumericUserNames = false,
        RequireUniqueEmail = true
    };
    manager.UserLockoutEnabledByDefault = true;
    manager.DefaultAccountLockoutTimeSpan = new TimeSpan(0, 20, 0);
    manager.MaxFailedAccessAttemptsBeforeLockout = 5;
    // Configure validation logic for passwords
    manager.PasswordValidator = new PasswordValidator
    {
        RequiredLength = 6,
        RequireNonLetterOrDigit = false,
        RequireDigit = true,
        RequireLowercase = true,
        RequireUppercase = true,
    };
    // Register two factor authentication providers. This application uses Phone and Emails as a step
    // You can write your own provider and plug in here.
    manager.RegisterTwoFactorProvider("PhoneCode", new PhoneNumberTokenProvider<ApplicationUser>
    {
        MessageFormat = "Your security code is: {0}"
    });
    manager.RegisterTwoFactorProvider("EmailCode", new EmailTokenProvider<ApplicationUser>
    {
        Subject = "Security Code",
        BodyFormat = "Your security code is: {0}"
    });
    manager.EmailService = new EmailService();
    manager.SmsService = new SmsService();

    return manager;
}
```

Prueba que las contraseñas se guardan hasheadas en base de datos

En la imagen se puede ver que las contraseñas no se guardan en base de datos como texto plano, si no que se guardan hasheadas, para mayor seguridad.

The screenshot shows a SQL Server Enterprise Manager interface. On the left, the 'Object Explorer' shows a database named 'HRAuthDB'. The main window displays a table with columns: 'id', 'Email', 'EmailConfirmed', 'PasswordHash', 'SecurityStamp', 'PhoneNumber', and 'PhoneNumberConfirmed'. The 'PasswordHash' column contains various alphanumeric strings, indicating that passwords are stored as hashes. A red box highlights the 'PasswordHash' column.

id	Email	EmailConfirmed	PasswordHash	SecurityStamp	PhoneNumber	PhoneNumberConfirmed
46d3deab6901cd	03629756C@no...	False	AfuaQ+YTkj8V0eyJgpa+kE0K1KAD4IR...	c10422-85d3...	NULL	False
016a7277-4e02...	Y5267946F@no...	False	AGpeQV6z2+QyyYiRa5SmY0a8k6wWpuf...	e070e0-710b...	NULL	False
018f2361-2380...	4012948A@no...	False	AfM4P9H0me5ajQPRfeyT0pHfE0woTen...	91c095-9a1c...	NULL	False
01870ca5-579a...	42097994@no...	False	ABEA9CFYwz7M0m7+ywECCVd3wCh3...	5aac70-d35a...	NULL	False
02615074-fad1...	34765630@no...	False	ALCBV7pMEnjad7YWM4gjj0paw0H8aE...	138896-0414...	NULL	False
02683343-95b2...	0079548T@no...	False	AfE0DgE+qj49i0m3QUH7ZHyGe/yHb5y...	57803b-923...	NULL	False
02a741c1-ceef...	4470707F@no...	False	AfBnA0v0a050N6v0d8Z0P7u0R00y5...	955391-670...	NULL	False
02a9606a-felb...	53366065Y@no...	False	ADp0R6Q2F8Nw70880M0ay2VHfM0q20...	184168-4e15...	NULL	False
02a95f4d-a303...	0533845C@no...	False	AfUA76ZDD0m-W+KpHUK8Wwly0T0qf...	1f5145-d56...	NULL	False
02b05ca-2022...	30995088F@no...	False	AB9F9mC70KZMa10D791CPy0gPH0cA...	338904-142...	NULL	False
02c22892-790c...	40997411H@no...	False	AEE+bbQmRfHfMcPF5+nK0U2gZi+fw...	09f010-070...	NULL	False
031187e-6d8b...	59963368T@no...	False	AfR0xh1-m82H63w70bqD4u8K00Mj...	c2b209-606...	NULL	False
0366cfe-3e1d...	33574235P@no...	False	AfHCYvCMTL9M6VYeK0X0a0p0+k0j0K...	d50668-774...	NULL	False
038fc4d7-820b...	01923459G@no...	False	AfA0v7DEtAnd5X0cVnK0c0B0V0D0a0Z...	077420-073...	NULL	False
03fa209c-7000...	16230504K@no...	False	ACA0LTK47vWnMk07uYHC4-BaHfWfEh...	ee31e5-ae3...	NULL	False
052e0372-f913...	37207062Z@no...	False	AEH6BHC13w0j0e8U0N0F46y0FAA0ygm...	190901-d87...	NULL	False
053eae1c-c009...	18047206V@no...	False	AAaY0gCNCVZB3H0h3qGm3P55VFC3C3...	c74ff7c-70c...	NULL	False
05740402-2746...	10101010P@no...	False	APNvUd0gjucc3j0u0D0B1M04E030V10p...	7cd072-600...	NULL	False
0579154b-3204...	54123466G@no...	False	AfHd5m00vB0Agm0gYfMv5er0Lu0Fek...	a5m7af-d5a...	NULL	False
0593b24c-499f...	4789551E@no...	False	AfZWBWmrcT5Qc3h3H1hg0Cp45j0vT0L...	7d0590-c17...	NULL	False
05d4990b-2414...	40578509B@no...	False	AAAz+I0vVW0U0CLA+0kVY0Z0v0c0RE...	64593c-019...	NULL	False
0609b761-d8a0...	26747700B@no...	False	AcvM4w03w+4ab0UpTyyMCC06H0j0B0S...	d37ca07-417...	NULL	False
06c991e-d254...	3840111E@no...	False	ADkMh1u8V0CLT0N+6A76P00U0R0RE...	0075eb6-a0f...	NULL	False
06f609f-b68e-4...	70485099Z@no...	False	AfMCA0eP5vNw35m0V97C+HhY0CvN7PA...	45d0927c-05...	NULL	False
07324001-571b...	20105032S@no...	False	AfX0kVw+ZjP50vWn1R0pQ0H0c0k0a0E0...	c36129b6-204...	NULL	False
076533b7-70e5...	54123472X@no...	False	Aa0b0v7Rw0h2v03dZV0BYfA0U0P0e0C...	3363768-00b...	NULL	False
0813951c-78b2...	55001144W@no...	False	AfE0H0TR0p0UP0Am0GZj0Lk0vWV0v0L...	346A0a7-3f3...	NULL	False
08718313-1a0c...	882808700@no...	False	AcYv573eEK0u01A84gH33YndK0oH0m7E...	48ac04b-95f...	NULL	False
08dc3bae-d47b...	7893052B@no...	False	AM0bt0d+044Ry/CgA0Tan0ZEFIAkYH0p0F...	b0a461a-524...	NULL	False
08fad369-ae1c...	50201037H@no...	False	ACd0dMDV0f0m0C0uM0a0F12z04H0L0...	ee03ab54-093...	NULL	False

Prueba de la política de sesiones inactivas

En la imagen se puede ver el código que limita el tiempo de inactividad de la sesión antes de considerarla como expirada.

```
public void ConfigureAuth(IApplicationBuilder app)
{
    // Configure the db context and user manager to use a single instance per request
    app.CreatePerOwinContext<ApplicationDbContext>().Create();
    app.CreatePerOwinContext<ApplicationUserManager>().Create();

    // Enable the application to use a cookie to store information for the signed in user
    // and to use a cookie to temporarily store information about a user logging in with a third party login provider
    // Configure the sign in cookie
    app.UseCookieAuthentication(new CookieAuthenticationOptions
    {
        AuthenticationType = DefaultAuthenticationTypes.ApplicationCookie,
        LoginPath = new PathString("/Account/Login"),
        Provider = new CookieAuthenticationProvider
        {
            OnValidateIdentity = SecurityStampValidator.OnValidateIdentity<ApplicationUserManager, ApplicationUser>(
                validateInterval: TimeSpan.FromMinutes(20),
                regenerateIdentity: (manager, user) => user.GenerateUserIdentityAsync(manager)
            ),
        },
        ExpireTimeSpan = TimeSpan.FromMinutes(20)
    });
}
```

Política de backup de los datos de nuestros clientes

De manera estándar se realizan copias de seguridad de la infraestructura virtual del cliente (hardware virtual) mediante el método de *snapshot*. Estas copias de seguridad permiten recuperar una máquina de forma rápida.

La periodicidad de la realización de copias de seguridad de manera estándar y sus **periodos de retención**

se explican a continuación:

- se realizará una copia de seguridad mediante el método de *snapshot* cada noche;
- se guardarán las copias de seguridad de los últimos 14 días;

Gestión de comunicaciones y operaciones

La política de seguridad relativa a la gestión de comunicaciones y operaciones se basa en las siguientes partes:

- asegurar el funcionamiento correcto y seguro de los sistemas de información;
- implantar y mantener el nivel apropiado de seguridad de la información en la provisión de servicios, manteniendo la consonancia con los posibles acuerdos de provisión de servicios de terceros;
- minimizar el riesgo de fallos de los sistemas;
- proteger la integridad del software y de la información;
- mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información;
- asegurar la protección de la información en las redes y la protección de la infraestructura de soporte;
- evitar la revelación, modificación, retirada o destrucción no autorizada de activos, y la interrupción de las actividades de los clientes;
- mantener la seguridad de la información y del software intercambiado dentro de la organización y con un tercero;
- detectar las actividades de procesamiento de información no autorizadas.

Plan de continuidad de negocio

Establece las acciones necesarias, y los responsables de llevarlas a cabo, para que la organización pueda recuperarse de incidentes de gravedad, tales como robos, incendios, terremotos, inundaciones, etc., con la mayor brevedad posible.

Estas acciones y sus responsables quedan fuera del alcance de este documento para evitar transmitir información confidencial.

Certificaciones de seguridad y valor añadido

Contamos con un SGSI (Sistema de Gestión de Seguridad de la Información) de acuerdo a las buenas prácticas que marca la norma ISO 27000.

Tenemos planificado la obtención de la certificación por la norma UNE/ISO 27001 para el presente año. Además, contamos con personal con certificaciones ISACA, CCIE.

Cumplimiento legal

En Rosclar cumplimos con la normativa legal vigente, estando adaptados sus procesos y datos a la LOPD (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD).

ROSCLAR